Configuração total da rede: RV345P e Cisco Business Wireless usando a interface de usuário da Web

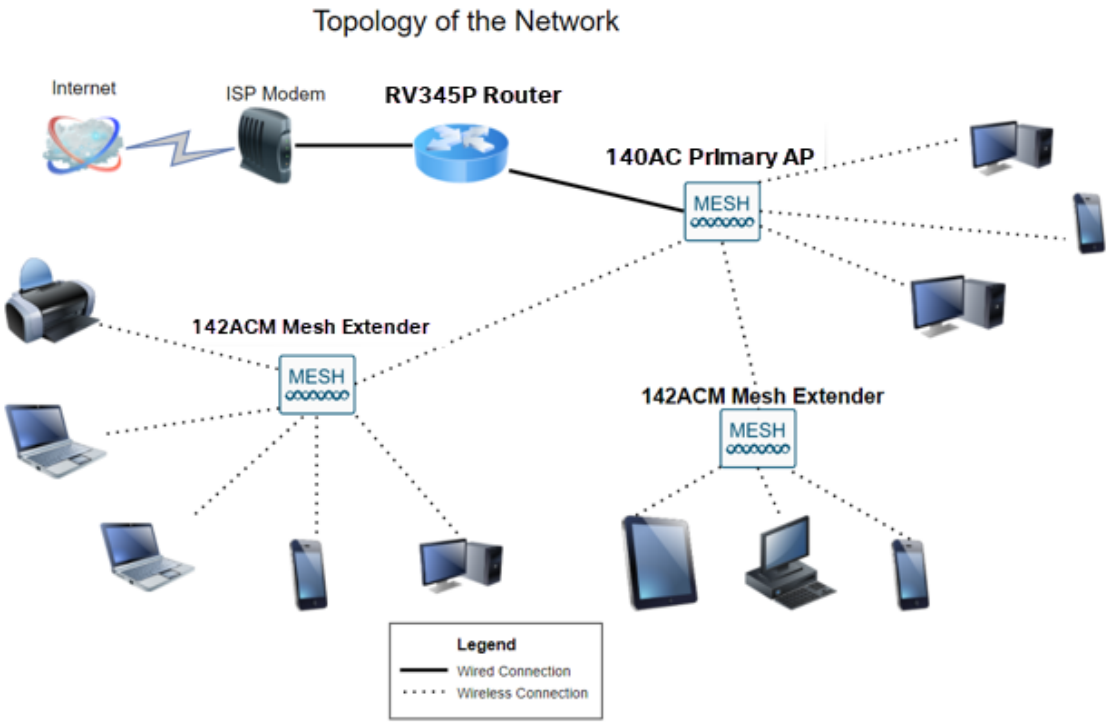
Objetivo

Este guia mostra como configurar uma rede de malha sem fio usando um roteador RV345P, um ponto de acesso CBW140AC e dois extensores de malha CBW142ACM.

Este artigo usa a interface de usuário da Web (UI) para configurar a rede sem fio em malha. Se preferir usar o aplicativo móvel, recomendado para fácil configuração sem fio, clique para ir para o artigo que usa o aplicativo móvel.

Table Of Contents

Topologia



Introduction

Toda a sua pesquisa se reuniu e você adquiriu seu equipamento da Cisco, que emocionante! Neste cenário, estamos usando um roteador RV345P. Este roteador fornece Power over Ethernet (PoE) que permite conectar o CBW140AC ao roteador em vez de um switch. Os extensores de malha CBW140AC e CBW142ACM serão usados para criar uma rede de malha sem fio.

Esse roteador avançado também oferece a opção para recursos adicionais.

1. O controle de aplicativos permite controlar o tráfego. Esse recurso pode ser configurado para permitir o tráfego, mas para registrá-lo, bloquear o tráfego e registrá-lo ou simplesmente bloquear o tráfego.
2. A filtragem da Web é usada para evitar que o tráfego da Web fique inseguro ou

impróprio para sites da Web. Não há registro com este recurso.

3. O AnyConnect é uma Rede Virtual Privada (VPN - Virtual Private Network) SSL (Secure Sockets Layer) disponível na Cisco. As VPNs permitem que usuários remotos e sites se conectem ao escritório da sua empresa ou a data centers fazendo um túnel seguro através da Internet.

Para usar esses recursos, você precisará comprar uma licença. Os roteadores e as licenças estão registrados online, o que será abordado neste guia.

Se você não está familiarizado com alguns dos termos usados neste documento ou deseja obter mais detalhes sobre a rede em malha, consulte os seguintes artigos:

- Negócios da Cisco: Glossário de novos termos
- Bem-vindo à rede em malha sem fio empresarial da Cisco
- Perguntas frequentes (FAQ) para uma rede sem fio empresarial da Cisco

Dispositivos aplicáveis | Versão do software

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0 (é necessário pelo menos um extensor de malha para a rede de malha)

Prerequisites

Prepare o roteador

1. Verifique se você tem uma conexão atual com a Internet para configuração.
2. Entre em contato com o ISP (Internet Service Provider, Provedor de serviços de Internet) para saber as instruções especiais que ele tem ao usar o roteador RV345P. Alguns ISPs oferecem gateways com roteadores integrados. Se você tiver um gateway com um roteador integrado, talvez seja necessário desativar o roteador e passar o endereço IP da rede de longa distância (WAN) (o endereço de protocolo de Internet exclusivo que o provedor de Internet atribui à sua conta) e todo o tráfego de rede até o novo roteador.
3. Decida onde colocar o roteador. Se possível, você vai querer uma área aberta. Isso pode não ser fácil, pois você deve conectar o roteador ao gateway de banda larga (modem) do seu ISP (Provedor de serviços de Internet).

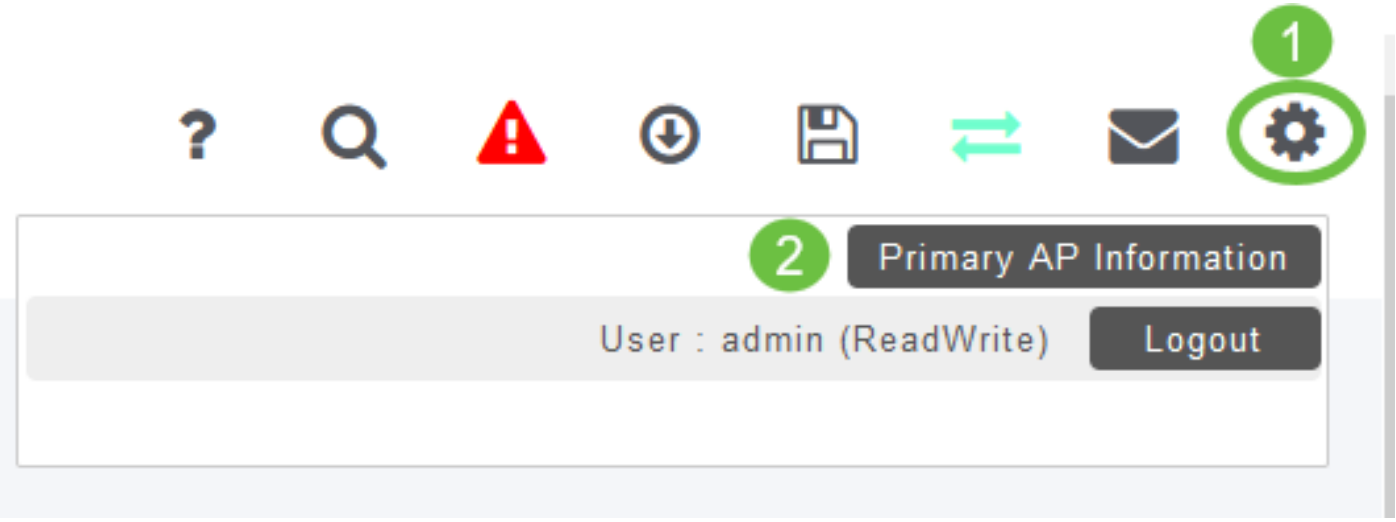
Obter uma conta no Cisco.com

Agora que você possui equipamentos da Cisco, é necessário obter uma conta do Cisco.com, às vezes chamada de identificação online do Cisco Connection (ID do CCO). Não há cobrança para uma conta.

Se você já tiver uma conta, poderá [ir para a próxima seção deste artigo](#).

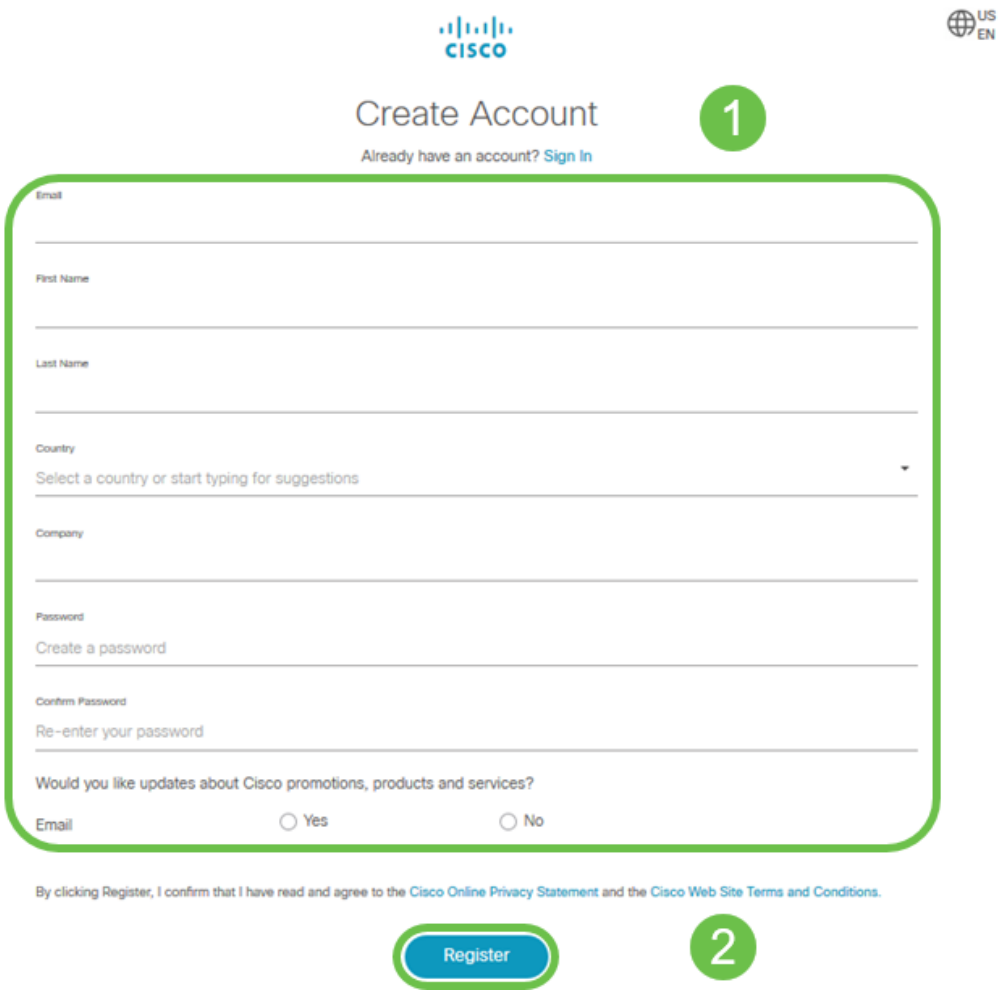
Passo 1

Vá para Cisco.com. Clique no **ícone de pessoa** e, em seguida, em **Criar uma conta**.



Passo 2

Insira os detalhes necessários para criar a conta e clique em **Registrar**. Siga as instruções para concluir o processo de registro.



Se tiver problemas, [clique para ir para a página de ajuda do registro de conta do](#)

Cisco.com.

Configurar o roteador RV345P

Um roteador é essencial em uma rede porque roteia pacotes. Permite que um computador se comunique com outros computadores que não estão na mesma rede ou sub-rede. Um roteador acessa uma tabela de roteamento para determinar para onde os pacotes devem ser enviados. A tabela de roteamento lista os endereços de destino. As configurações estáticas e dinâmicas podem ser listadas na tabela de roteamento para levar os pacotes ao seu destino específico.

O RV345P vem com configurações padrão otimizadas para muitas pequenas empresas. No entanto, suas demandas de rede ou ISP (Provedor de serviços de Internet) podem exigir que você modifique algumas dessas configurações. Depois de entrar em contato com o ISP para saber quais são os requisitos, você pode fazer alterações usando a interface do usuário da Web (UI).

Você está pronto? Vamos lá!

RV345P pronto para uso

Passo 1

Conecte o cabo Ethernet de uma das portas RV345P LAN (Ethernet) à porta Ethernet no computador. Você precisará de um adaptador se o computador não tiver uma porta Ethernet. O terminal deve estar na mesma sub-rede com fio que o RV345P para executar a configuração inicial.

Passo 2

Não se esqueça de usar o adaptador de alimentação fornecido com o RV345P. O uso de um adaptador de energia diferente pode danificar o RV345P ou fazer com que os dongles USB falhem. Por padrão, a chave liga/desliga está ligada.

Conecte o adaptador de alimentação à porta 12VDC do RV345P, mas ainda não o conecte à alimentação.

Etapa 3

Verifique se o modem está desligado.

Passo 4

Use um cabo Ethernet para conectar o modem a cabo ou DSL à porta WAN no RV345P.

Etapa 5

Conecte a outra extremidade do adaptador RV345P a uma tomada elétrica. Isso ligará o RV345P. Reconecte o modem para que ele possa ser ligado também. A luz de alimentação no painel frontal fica verde estável quando o adaptador de energia está conectado corretamente e o RV345P está concluído na inicialização.

Configurar o roteador

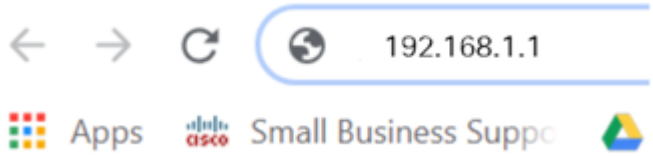
O trabalho preparatório está pronto, agora é hora de chegar a algumas configurações! Para iniciar a IU da Web, siga estes passos.

Passo 1

Se seu computador estiver configurado para se tornar um cliente DHCP (Dynamic Host Configuration Protocol), um endereço IP no intervalo 192.168.1.x será atribuído ao PC. O DHCP automatiza o processo de atribuição de endereços IP, máscaras de sub-rede, gateways padrão e outras configurações para computadores. Os computadores devem ser configurados para participar do processo DHCP para obter um endereço. Isso é feito selecionando-se para obter um endereço IP automaticamente nas propriedades do TCP/IP no computador.

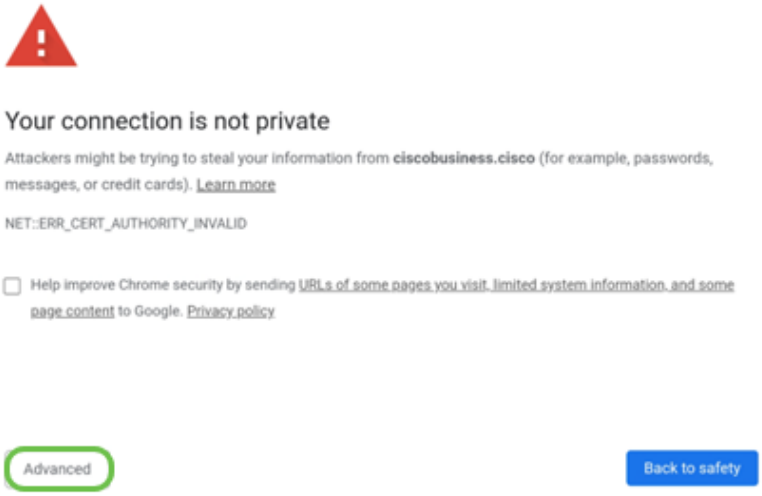
Passo 2

Abra um navegador da Web, como Safari, Internet Explorer ou Firefox. Na barra de endereços, insira o endereço IP padrão do RV345P, 192.168.1.1.



Etapa 3

O navegador pode emitir um aviso de que o site não é confiável. Continue no site. Se você não estiver conectado, vá para Solução de problemas da conexão com a Internet .

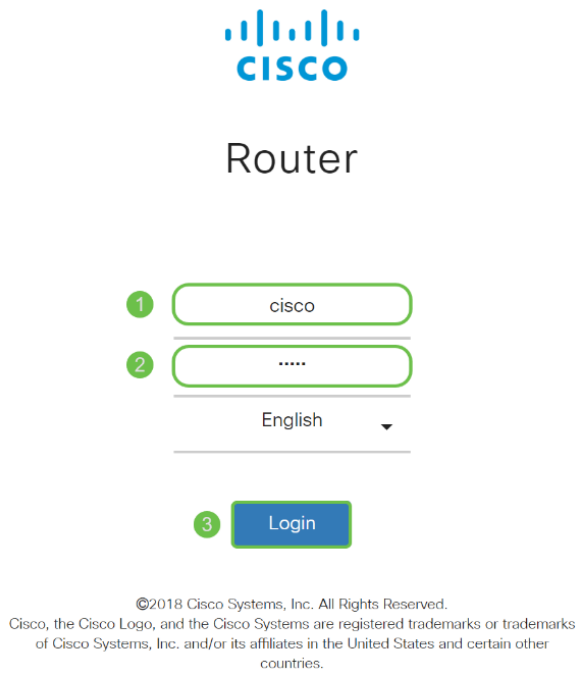


Passo 4

Quando a página de entrada for exibida, digite o nome de usuário padrão *cisco* e a senha padrão *cisco*.

Clique em login.

Para obter informações detalhadas, clique em How to access the web-based setup page of Cisco RV340 series VPN routers.



Etapa 5

Clique em login. A página *Guia de introdução* é exibida. Se o painel de navegação não estiver aberto, você pode abri-lo clicando no **ícone de menu**.

Agora que você confirmou a conexão e fez login no roteador, vá para a seção Configuração inicial deste artigo.

Solução de problemas da conexão com a Internet

Se você estiver lendo isso, provavelmente está tendo problemas para se conectar à Internet ou à IU da Web. Uma dessas soluções deve ajudar.

No SO Windows conectado, você pode testar a conexão de rede abrindo o prompt de comando. Insira **ping 192.168.1.1** (o endereço IP padrão do roteador). Se a solicitação expirar, você não poderá se comunicar com o roteador.

Se a conectividade não estiver acontecendo, você pode conferir este artigo Solução de problemas.

Algumas outras coisas para tentar:

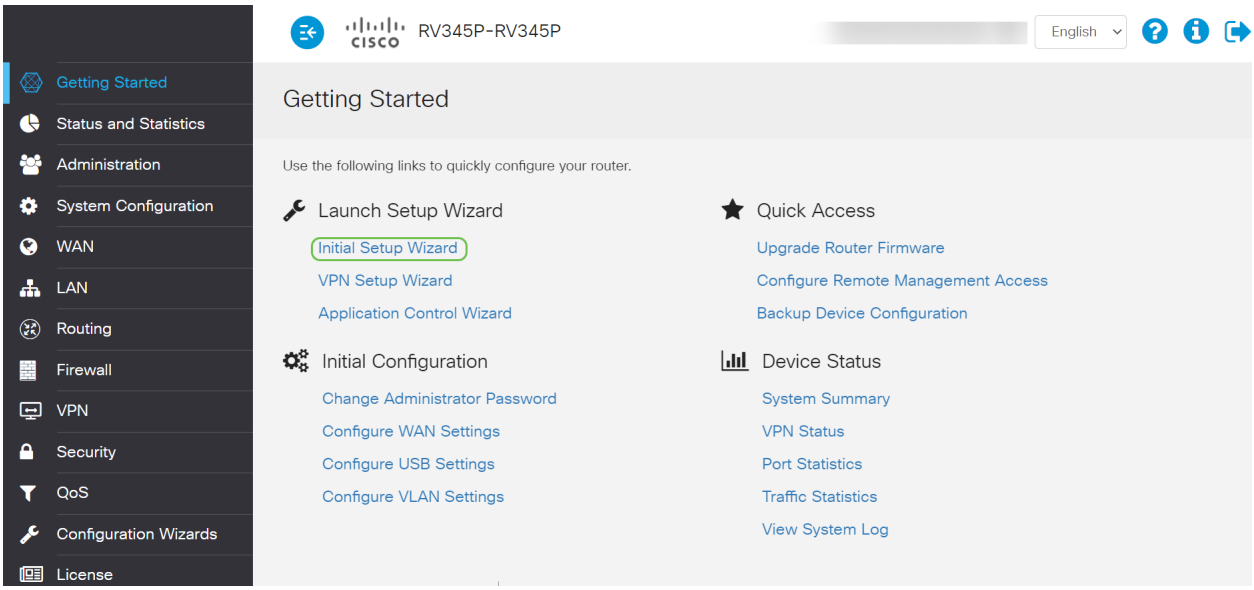
1. Verifique se o navegador da Web não está definido como Trabalhar off-line.
2. Verifique as configurações de conexão de rede local do adaptador Ethernet. O PC deve obter um endereço IP por meio do DHCP. Como alternativa, o PC pode ter um endereço IP estático no intervalo 192.168.1.x com o gateway padrão definido como 192.168.1.1 (o endereço IP padrão do RV345P). Para se conectar, talvez seja necessário modificar as configurações de rede do RV345P. Se estiver usando o Windows 10, verifique as instruções do Windows 10 para modificar as configurações de rede.
3. Se você tiver um equipamento existente ocupando o endereço IP 192.168.1.1, será necessário resolver esse conflito para que a rede funcione. Mais sobre isso no final desta seção, ou clique aqui para ser levado diretamente.
4. Redefina o modem e o RV345P desligando ambos os dispositivos. Em seguida, ligue o modem e deixe-o ocioso por cerca de 2 minutos. Em seguida, ligue o RV345P. Agora você deve receber um endereço IP WAN.
5. Se você tiver um modem DSL, peça ao ISP para colocar o modem DSL no modo bridge.

Configuração inicial

Recomendamos que você passe pelas etapas do *Assistente de configuração inicial* listadas nesta seção. Você pode alterar essas configurações a qualquer momento.

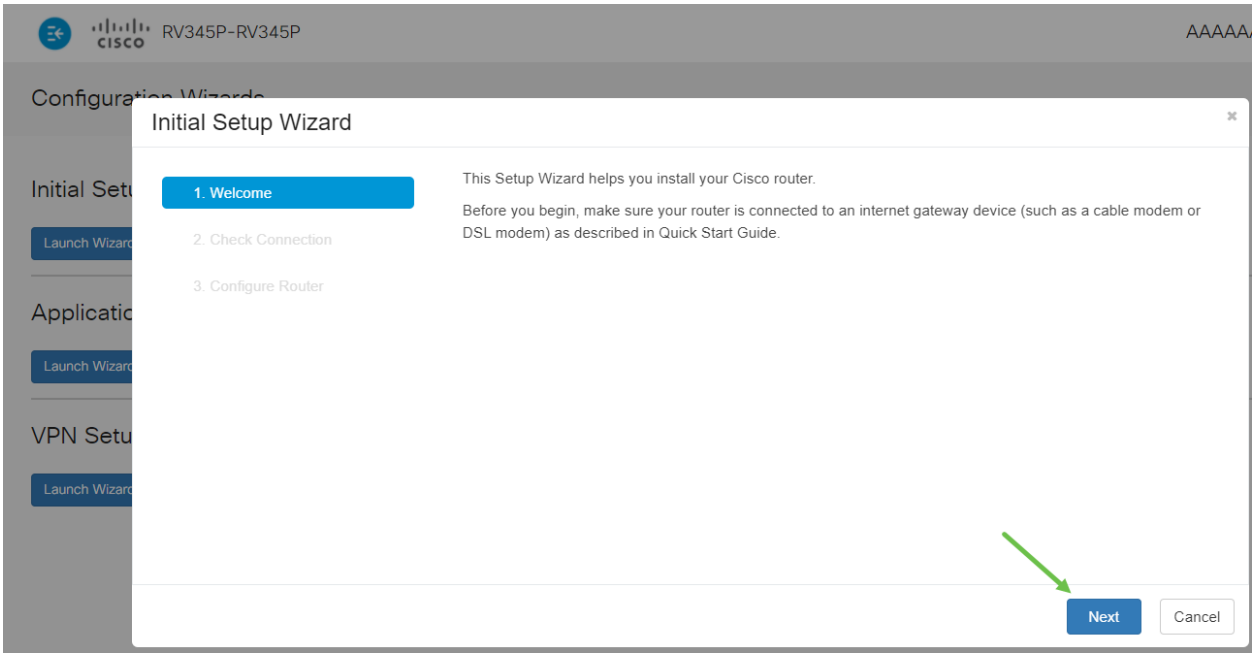
Passo 1

Clique em **Assistente de configuração inicial** na página *Introdução*.



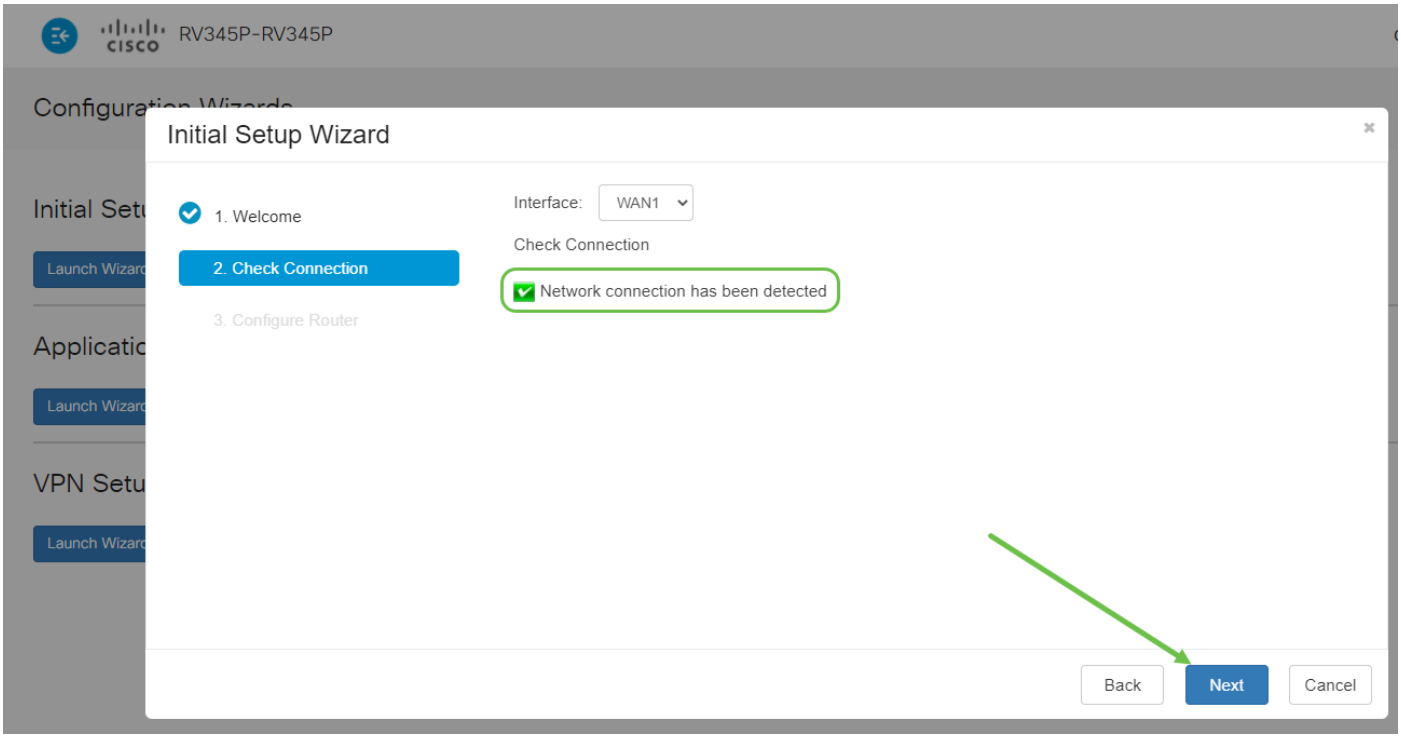
Passo 2

Esta etapa confirma se os cabos estão conectados. Como você já confirmou isso, clique em **Avançar**.



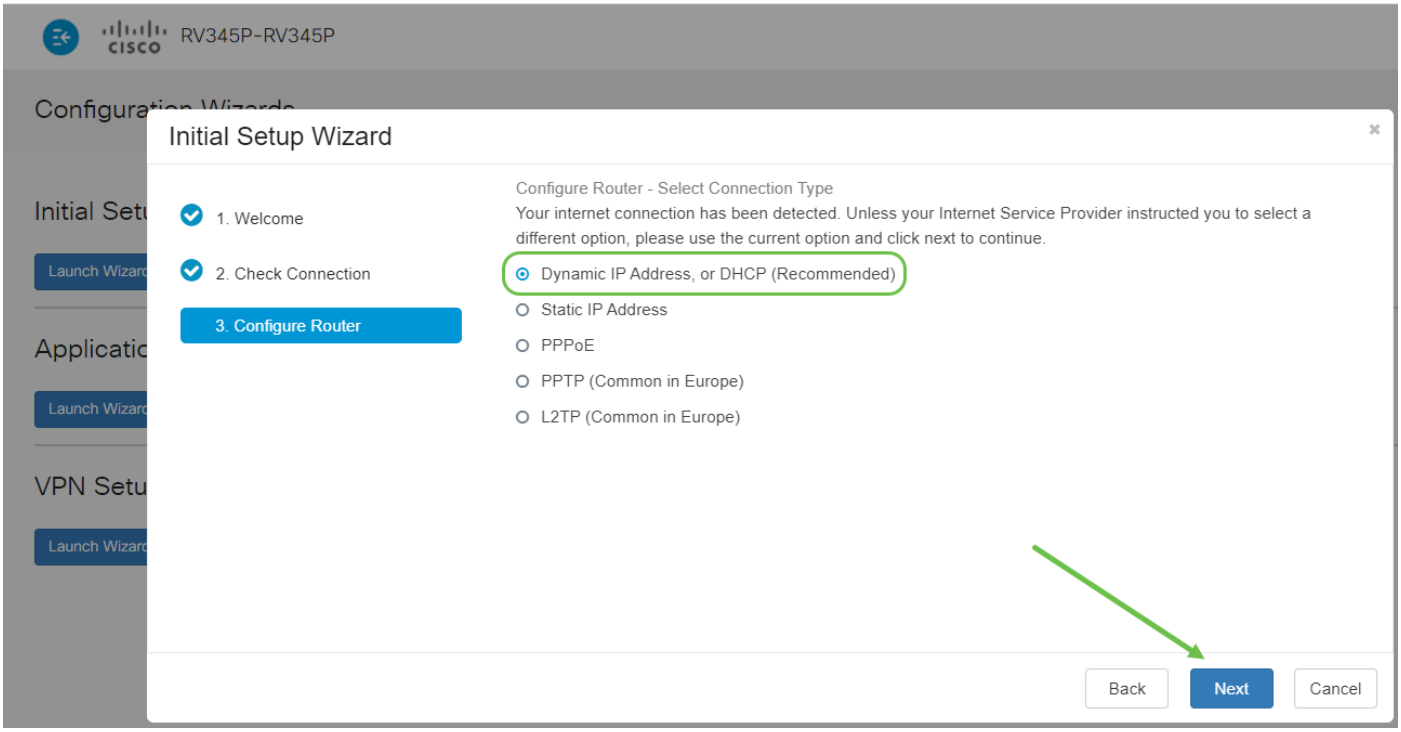
Etapa 3

Esta etapa aborda as etapas básicas para garantir que o roteador esteja conectado. Como você já confirmou isso, clique em **Avançar**.



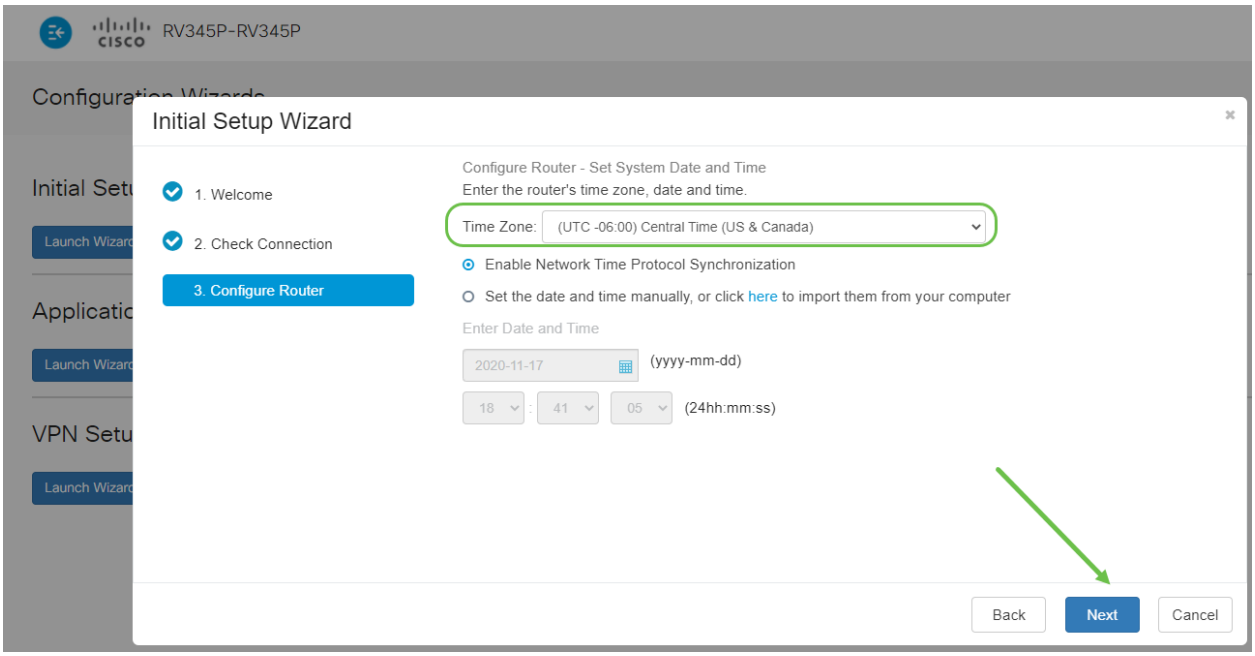
Passo 4

A próxima tela exibe suas opções para atribuir endereços IP ao roteador. Você precisa selecionar DHCP neste cenário. Clique em Next.



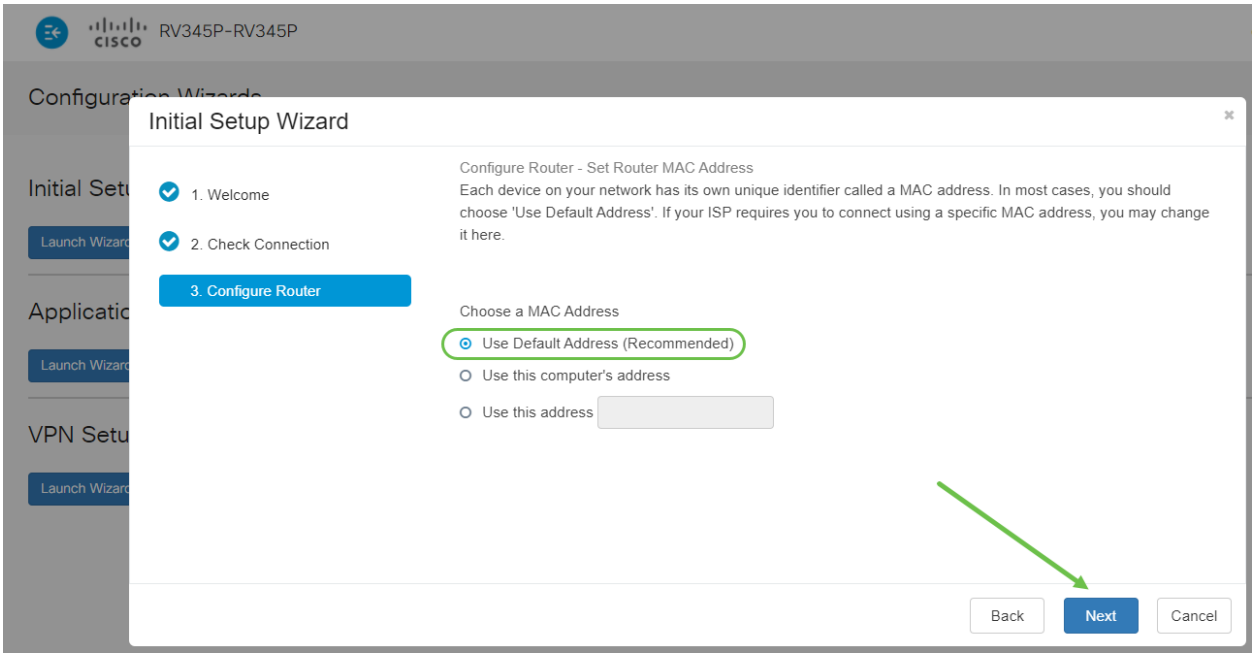
Etapa 5

Você será solicitado a definir as configurações de hora do roteador. Isso é importante porque permite precisão ao revisar logs ou eventos de solução de problemas. Selecione seu **fuso horário** e clique em **Avançar**.



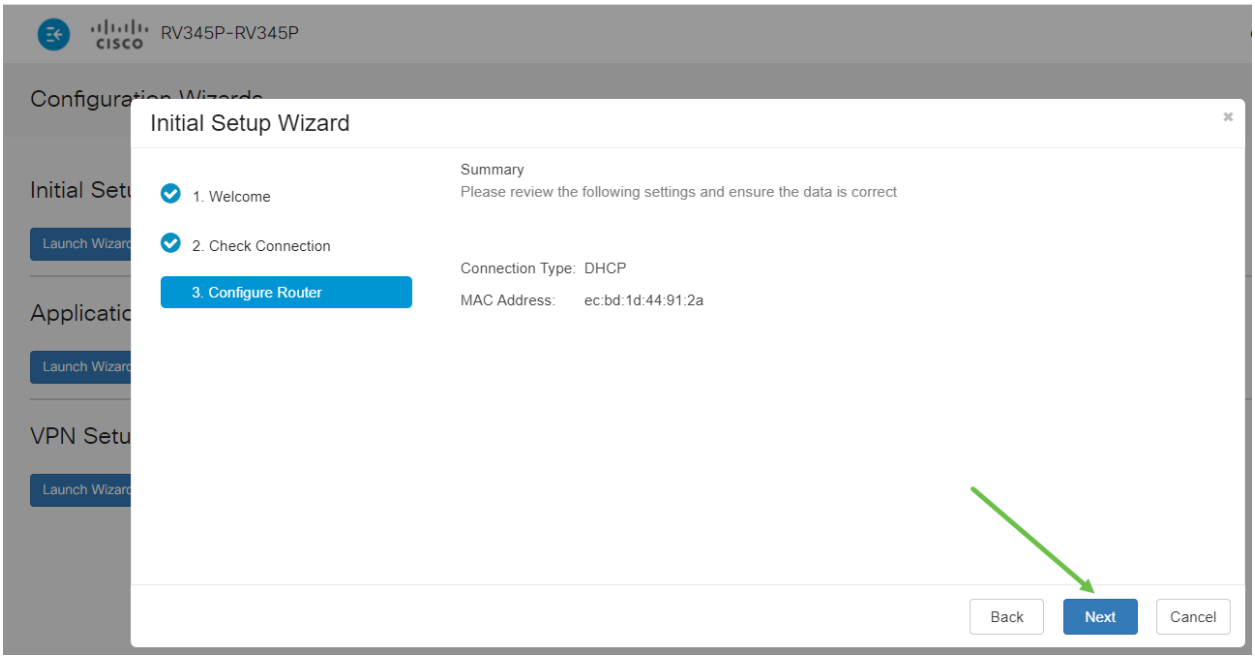
Etapa 6

Você selecionará os endereços MAC a serem atribuídos aos dispositivos. Com mais frequência, você usará o endereço padrão. Clique em Next.



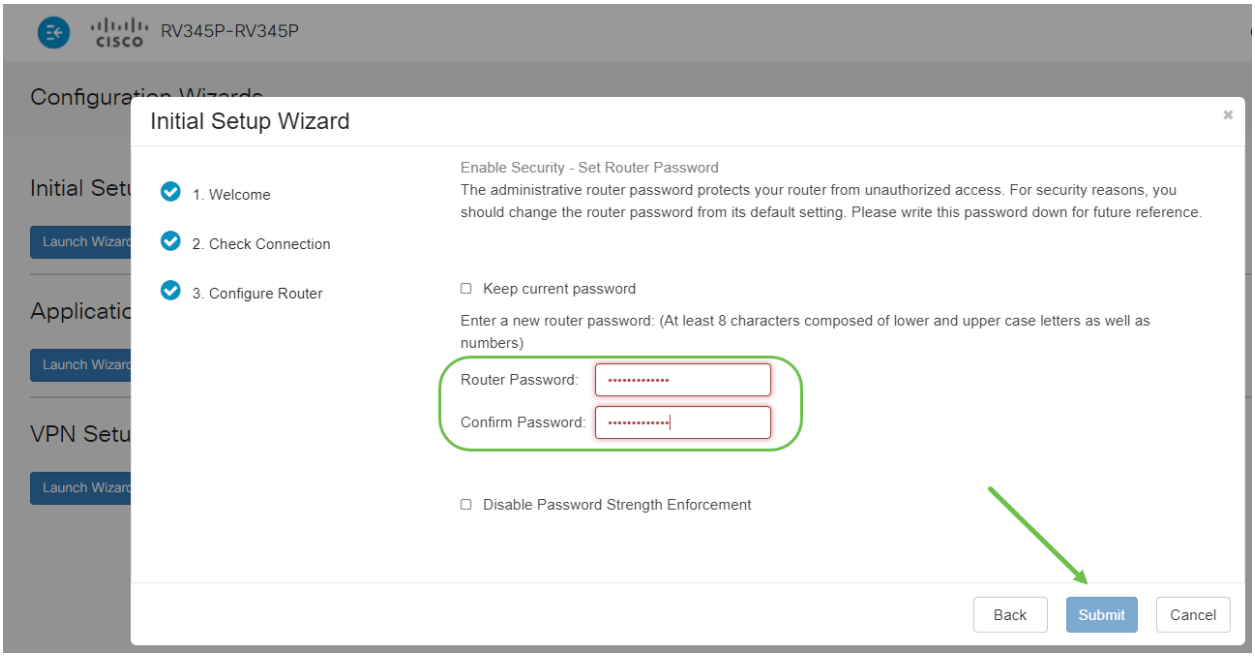
Etapa 7

A página a seguir é um resumo das opções selecionadas. Revise e clique em **Next (Avançar)** se satisfeito.



Passo 8

Na próxima etapa, você selecionará uma senha para usar ao fazer login no roteador. O padrão para senhas é conter pelo menos 8 caracteres (maiúsculas e minúsculas) e incluir números. **Digite uma senha** que esteja em conformidade com os requisitos de força. Clique em Next. Anote sua senha para logins futuros.



Não é recomendável selecionar Desativar *imposição de força da senha*. Essa opção permite que você selecione uma senha tão simples quanto 123, o que seria tão fácil quanto 1-2-3 para agentes mal-intencionados quebrarem.

Passo 9

Clique no **ícone salvar**.

Se quiser mais informações sobre essas configurações, você pode ler Configure DHCP WAN Settings no RV34x Router.

O RV345P tem Power over Ethernet (PoE) ativado por padrão, mas você pode fazer alguns ajustes. Se precisar personalizar as configurações, verifique Configurar as configurações de PoE (Power over Ethernet) no roteador RV345P.

Edite um endereço IP, se necessário (opcional)

Após concluir o *Assistente de configuração inicial*, você pode definir um endereço IP estático no roteador editando as configurações da VLAN.

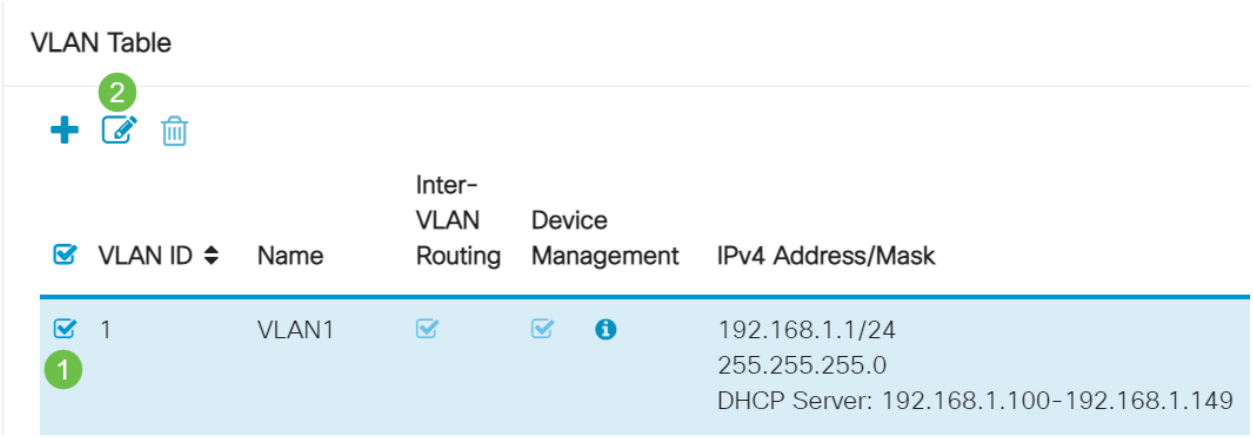
Esse processo só é necessário se o endereço IP do roteador precisar receber um endereço específico na rede existente. Se não precisar editar um endereço IP, você pode ir para a próxima seção deste artigo.

Passo 1

No menu à esquerda, clique em **LAN > VLAN Settings**.

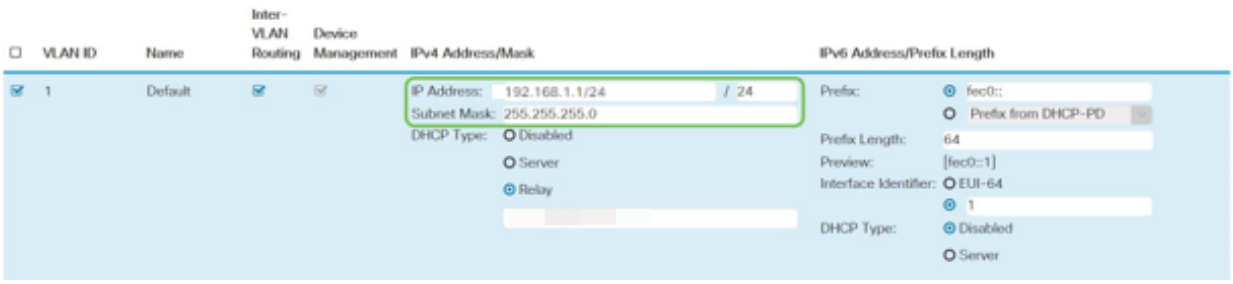
Passo 2

Selecione a **VLAN** que contém seu dispositivo de roteamento e clique no **ícone de edição**.



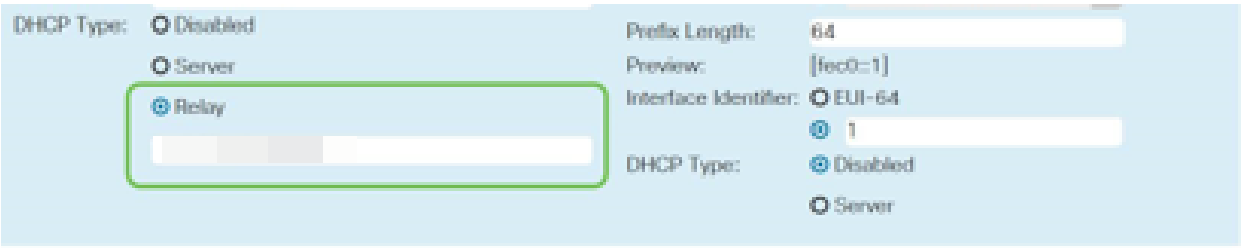
Etapa 3

Insira o **endereço IP estático** desejado e clique em **Apply (Aplicar)** no canto superior direito.



Etapa 4 (Opcional)

Se o roteador não for o servidor/dispositivo DHCP atribuindo endereços IP, você poderá usar o recurso de Retransmissão DHCP para direcionar solicitações DHCP a um endereço IP específico. O endereço IP provavelmente será o roteador conectado à WAN/Internet.

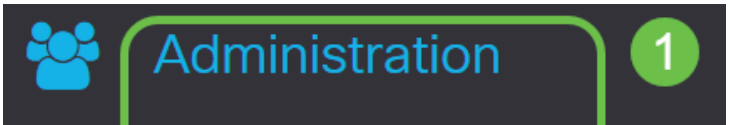


Atualize o firmware, se necessário

Essa é uma etapa importante, não pule!

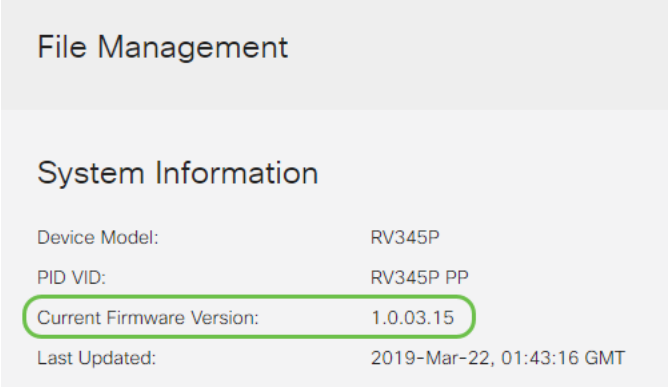
Passo 1

Escolha **Administration > File Management**.



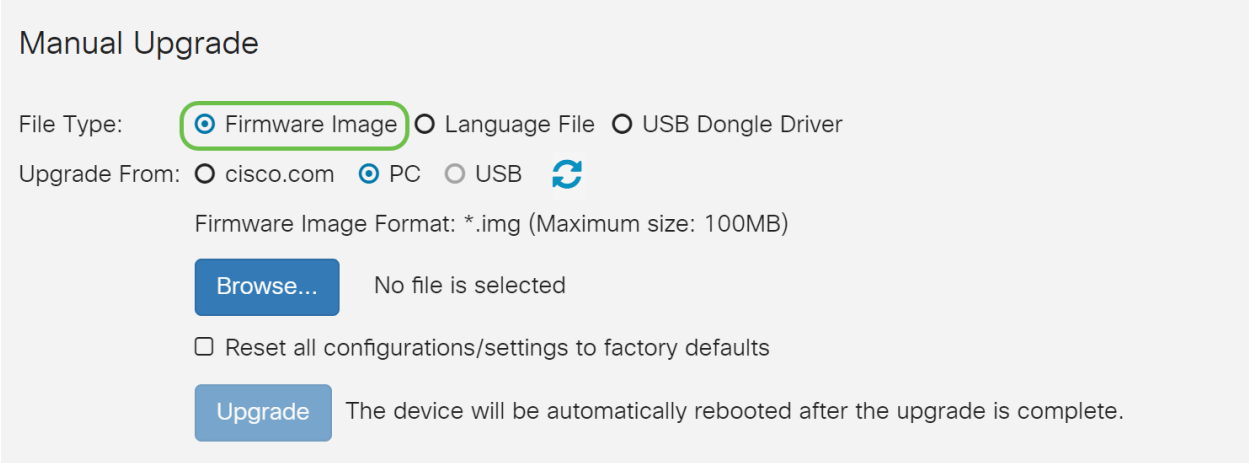
Na área *Informações do Sistema*, as seguintes subáreas descrevem o seguinte:

- Modelo do dispositivo - Exibe o modelo do dispositivo.
- PID VID - ID do produto e ID do fornecedor do roteador.
- Versão atual do firmware - Firmware que está sendo executado no momento no dispositivo.
- Versão mais recente disponível no Cisco.com - Versão mais recente do software disponível no site da Cisco.
- Última atualização do firmware - Data e hora da última atualização do firmware feita no roteador.



Passo 2

Na seção *Atualização manual*, clique no botão de opção **Imagem do firmware** para *Tipo de arquivo*.



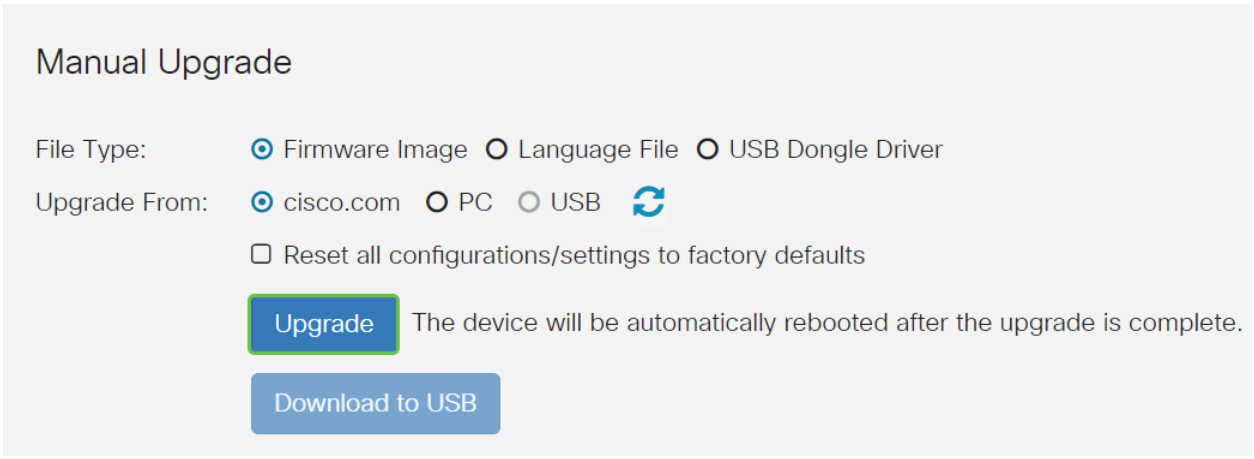
Etapa 3

Na página *Atualização manual*, clique no botão de opção para selecionar *cisco.com*. Há outras opções para isso, mas essa é a maneira mais fácil de fazer uma atualização. Este processo instala o arquivo de atualização mais recente diretamente da página da Web Downloads de software da Cisco.

Se o dispositivo não estiver conectado à Internet ou estiver sofrendo com desconexões da Internet, você não poderá atualizar a partir do cisco.com. Se isso se refere a você, opções alternativas podem ser encontradas aqui.

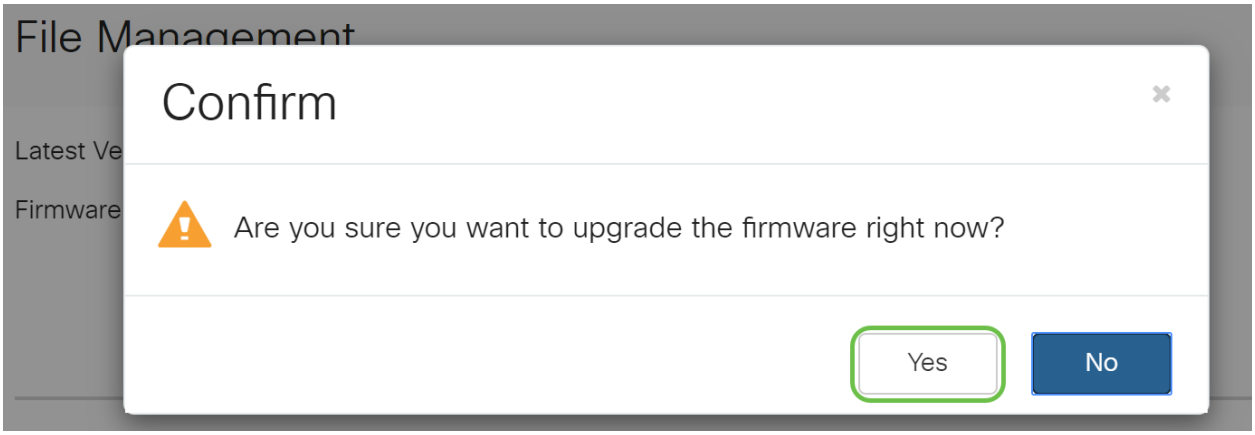
Passo 4

Clique em **Atualizar**.

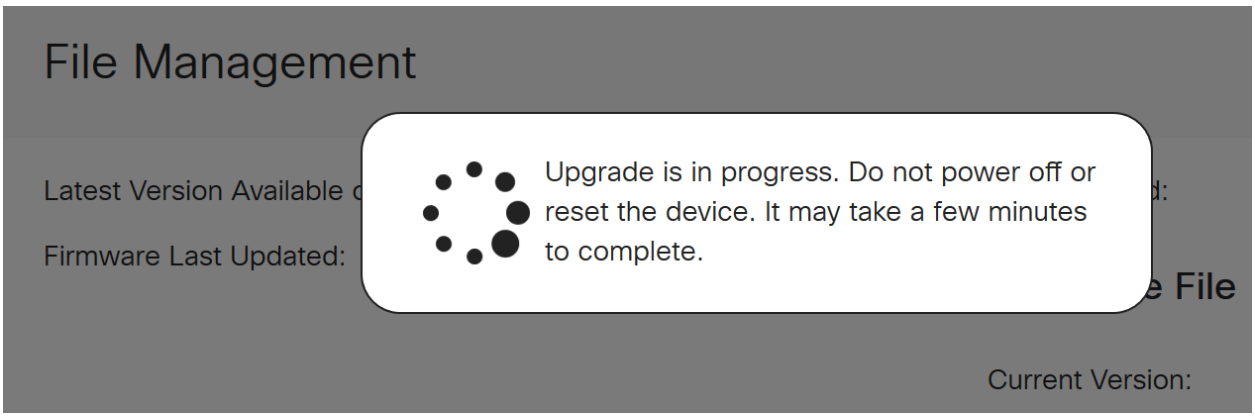


Etapa 5

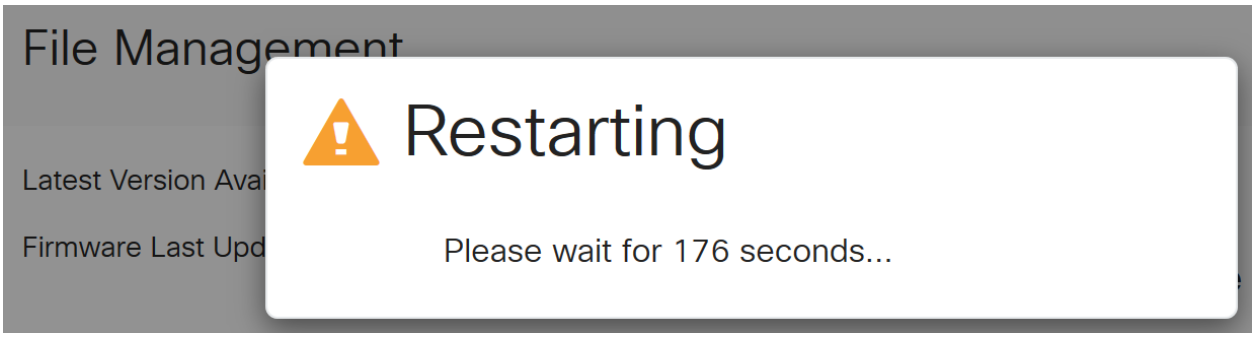
Clique em **Sim** na janela de confirmação para continuar.



O processo de atualização precisa ser executado sem interrupção. Você receberá a seguinte mensagem na tela enquanto a atualização estiver em andamento.

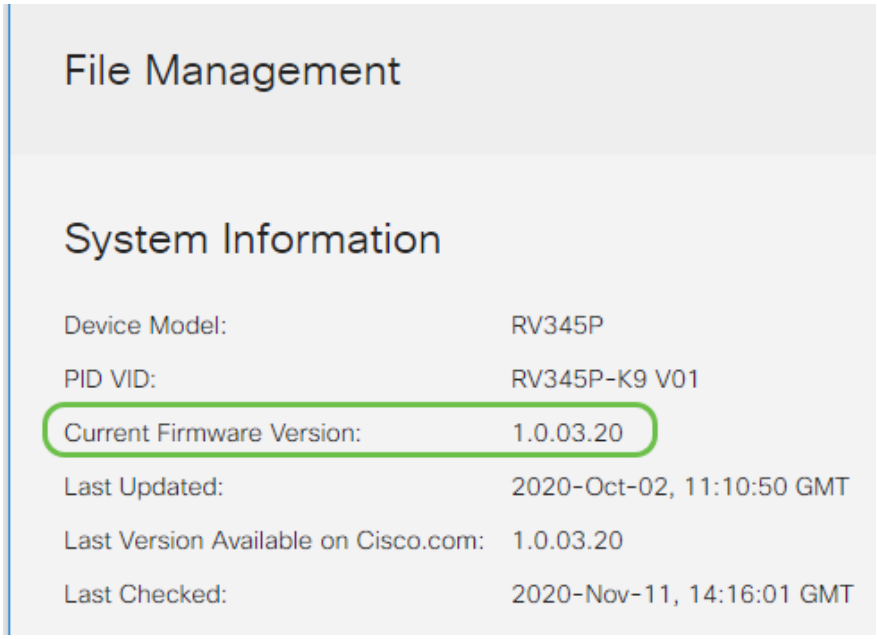


Quando a atualização for concluída, uma janela de notificação será exibida para informá-lo de que o roteador será *reinicializado* com uma contagem regressiva do tempo estimado para a conclusão do processo. Depois disso, você será desconectado.



Etapa 6

Efetue login novamente no utilitário baseado na Web para verificar se o firmware do roteador foi atualizado e vá até *System Information (Informações do sistema)*. A área *Versão atual do firmware* deve agora exibir a versão atualizada do firmware.

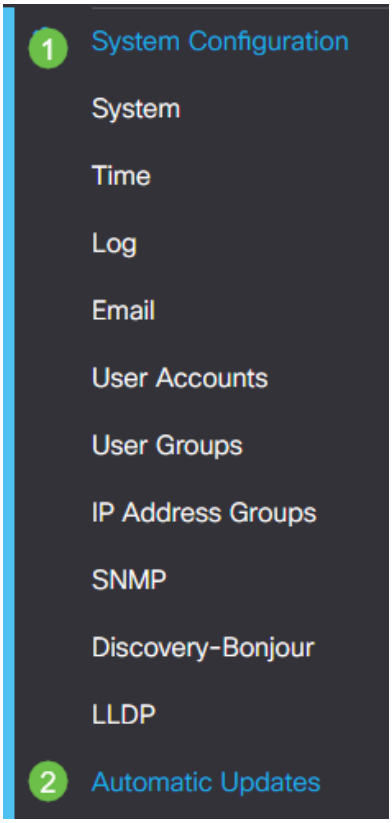


Configurar atualizações automáticas no roteador RV345P Series

Como as atualizações são tão importantes e você é uma pessoa ocupada, faz sentido configurar as atualizações automáticas daqui para fora!

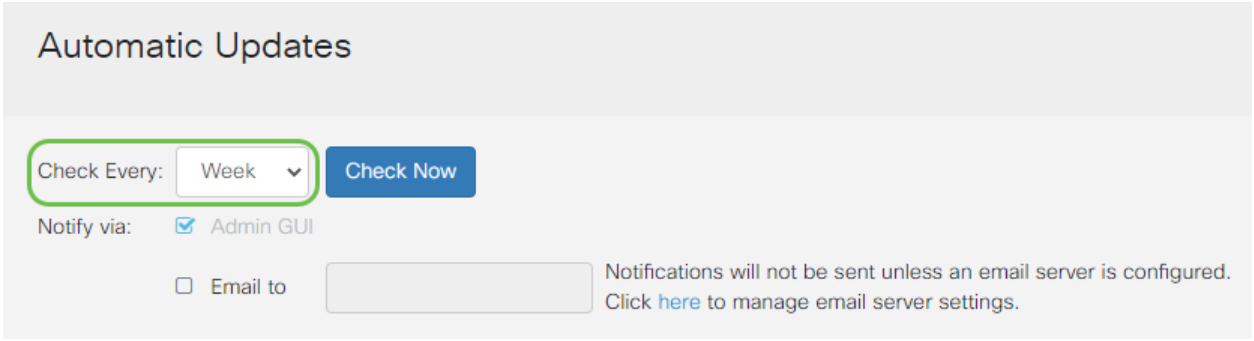
Passo 1

Efetue login no utilitário baseado na Web e escolha **System Configuration > Automatic Updates (Configuração do sistema > Atualizações automáticas)**.



Passo 2

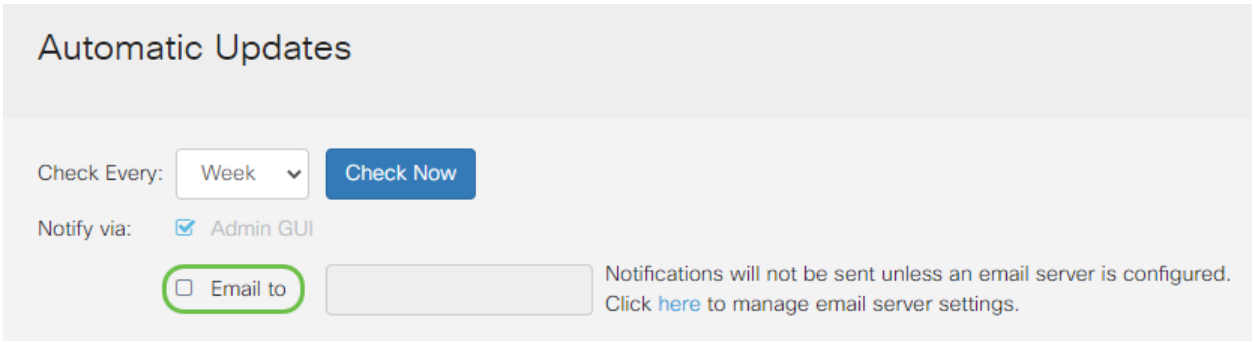
Na lista suspensa *Verificar cada*, escolha com que frequência o roteador deve procurar atualizações.



Etapa 3

Na área *Notificar via*, marque a caixa de seleção **Email to** para receber atualizações por e-mail. A caixa de seleção *da GUI do administrador* está habilitada por padrão e não pode ser desabilitada. Uma notificação aparecerá na configuração baseada na Web quando uma atualização estiver disponível.

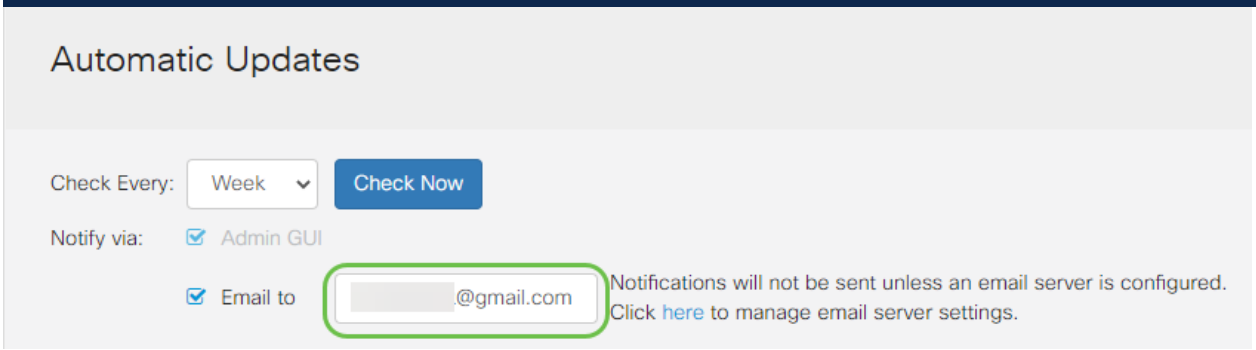
Para configurar as definições do servidor de correio eletrônico, clique aqui para saber como.



Passo 4

Insira um endereço de e-mail no campo *Email to address (E-mail para* endereço).

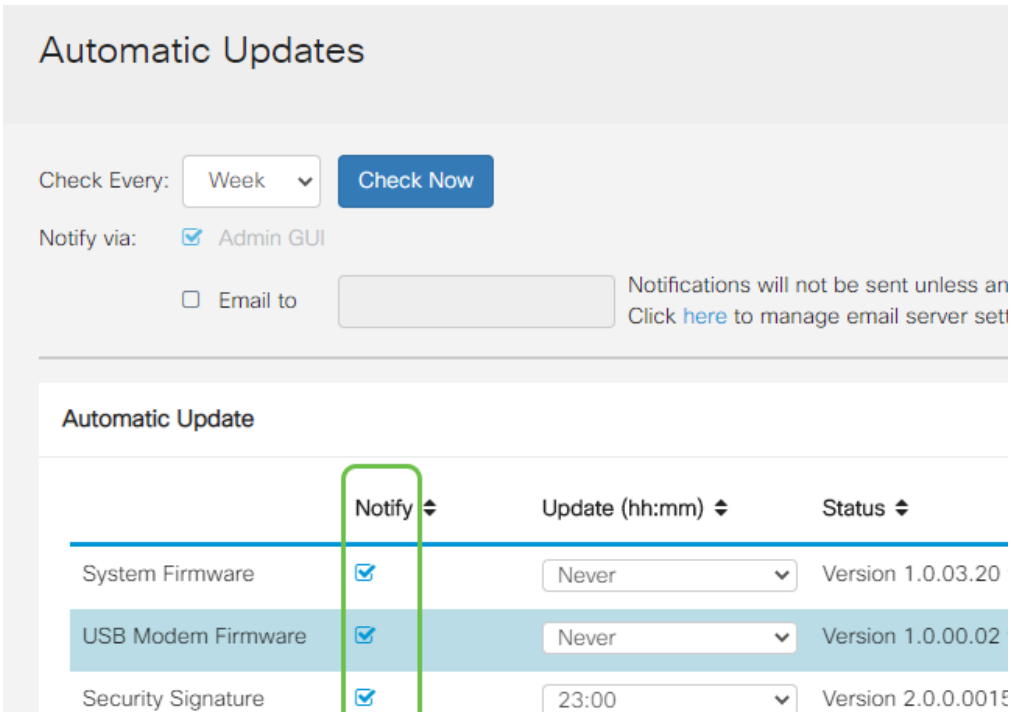
É altamente recomendável usar uma conta de e-mail separada em vez de usar seu e-mail pessoal para manter a privacidade.



Etapa 5

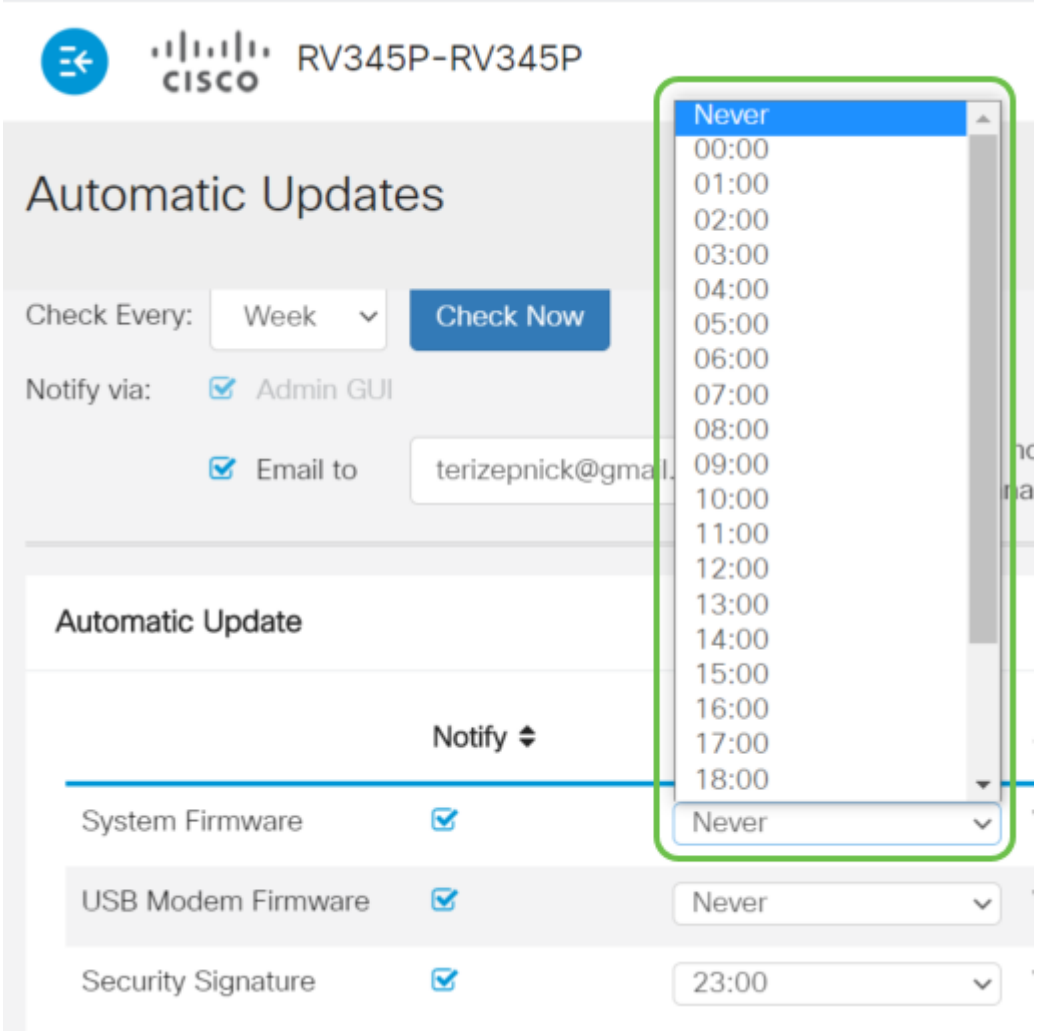
Na área *Atualização automática*, marque as caixas de seleção **Notificar** do tipo de atualização sobre a qual deseja ser notificado. As opções são:

- Firmware do sistema — O principal programa de controle do dispositivo.
- Firmware de modem USB — O programa de controle ou driver para a porta USB.
- Assinatura de segurança — Conterá assinaturas para o Controle de aplicativos para identificar aplicativos, tipos de dispositivos, sistemas operacionais e assim por diante.



Etapa 6

Na lista suspensa *Atualização automática*, escolha uma hora do dia em que deseja que a atualização automática seja feita. Algumas opções podem variar de acordo com o tipo de atualização escolhido. A assinatura de segurança é a única opção a ter uma atualização imediata. Recomenda-se que você defina um horário em que seu escritório seja fechado para que o serviço não seja interrompido em um momento inconveniente.



O status exibe a versão em execução no momento do firmware ou da assinatura de segurança.

Etapa 7

Clique em Apply.

Passo 8

Para salvar a configuração permanentemente, vá para a página Copiar/salvar configuração ou clique no **ícone salvar** na parte superior da página.

Incrível, suas configurações básicas no roteador estão completas! Agora você tem algumas opções de configuração para explorar.

Opções de segurança

Éclaro que você quer que sua rede esteja segura. Há algumas opções simples, como ter uma senha complexa, mas se você quiser tomar medidas para uma rede ainda mais segura, confira esta seção sobre segurança.

Licença de segurança RV (opcional)

Esta licença de segurança RV protege a sua rede de ataques da Internet:

- Sistema de prevenção de intrusão (IPS): Inspeciona pacotes, registros e/ou bloqueia uma ampla gama de ataques à rede. Ele oferece maior disponibilidade de rede, correção mais rápida e proteção abrangente contra ameaças.
- Antivírus: Proteção contra vírus, verificando os aplicativos em busca de vários protocolos, como HTTP, FTP, anexos de e-mail SMTP, anexos de e-mail POP3 e anexos de e-mail IMAP que passam pelo roteador.
- Segurança da Web: Permite a eficiência e a segurança da empresa, ao mesmo tempo em que se conecta à Internet, permite que as políticas de acesso à Internet para dispositivos finais e aplicativos de Internet ajudem a garantir o desempenho e a segurança. Ele é baseado em nuvem e contém mais de 80 categorias com mais de 450 milhões de domínios classificados.
- Identificação do aplicativo: Identificar e atribuir políticas a aplicativos da Internet. 500 aplicativos exclusivos são identificados automaticamente.
- Identificação do cliente: Identifique e categorize os clientes dinamicamente. A capacidade de atribuir políticas com base na categoria do dispositivo final e no sistema operacional.

A Licença de Segurança RV fornece Filtragem da Web. Filtragem da Web é um recurso que permite gerenciar o acesso a sites inadequados. Ele pode filtrar as solicitações de acesso à Web de um cliente para determinar se permite ou nega esse site.

Os recursos de segurança licenciados podem ser testados sem nenhum custo por 90 dias. Caso deseje continuar usando os recursos de segurança avançada em seu roteador após o período de avaliação, adquira e ative uma licença.

Outra opção de segurança é o Cisco Umbrella. Clique aqui se quiser ir para a seção Umbrella.

Se você não quiser uma licença de segurança, clique para ir para a seção VPN deste documento.

Introdução às Smart Accounts

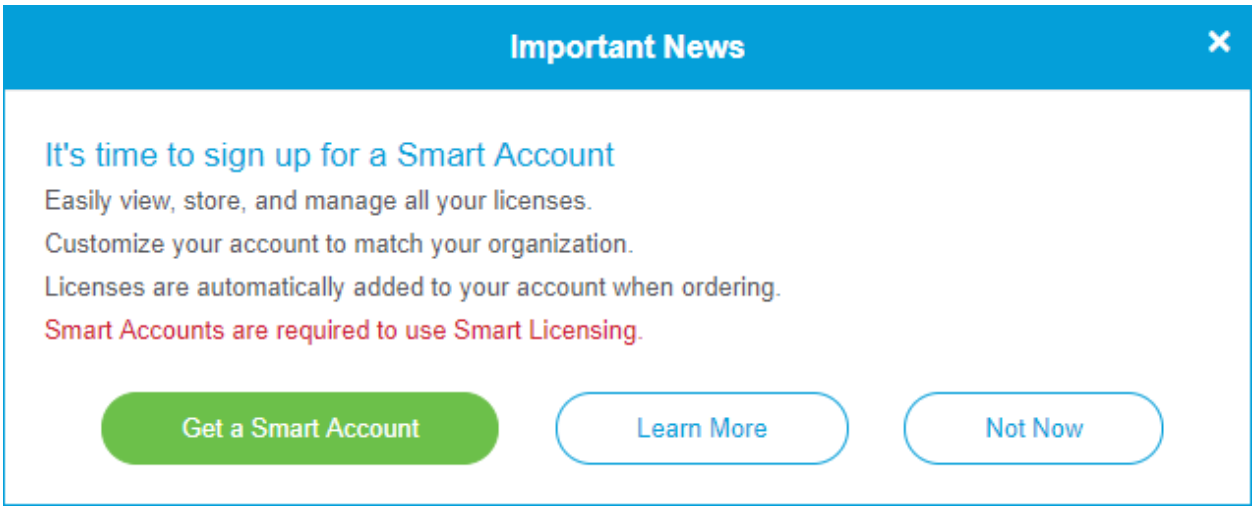
Para adquirir a licença de segurança RV, você precisa de uma Smart Account.

Ao autorizar a ativação desta Smart Account, você concorda que está autorizado a criar contas e gerenciar direitos de produtos e serviços, contratos de licença e acesso de usuário às contas em nome da sua organização. Os parceiros da Cisco não podem autorizar a criação de conta em nome dos clientes.

A criação de uma nova Smart Account é um evento único, e o gerenciamento desse ponto em diante é fornecido através da ferramenta.

Criar uma Smart Account

Quando você acessa sua conta geral da Cisco usando sua conta do Cisco.com, ou ID do CCO (a que você criou no início deste documento), pode ser saudado por uma mensagem para criar uma Smart Account.



Se ainda não viu esta janela pop-up, você pode clicar para ser levado à página de criação da Smart Account. Talvez seja necessário fazer login com suas credenciais de conta do Cisco.com.

Para obter mais detalhes sobre as etapas envolvidas na solicitação de sua Conta inteligente, clique aqui.

Anote o nome da sua conta e outros detalhes de registro.

Dica rápida: se você precisa inserir um domínio e não tem um, você pode inserir seu endereço de e-mail no formato de *name@domain.com*. Domínios comuns são gmail, yahoo, etc., dependendo da sua empresa ou provedor.

É muito importante que você tenha uma conta Cisco.com (CCO ID) e uma conta inteligente da Cisco antes de adquirir a licença de segurança RV.

Comprar licença de segurança RV

Você deve adquirir uma licença do seu distribuidor da Cisco ou do seu parceiro da Cisco. Para localizar um parceiro da Cisco, clique aqui.

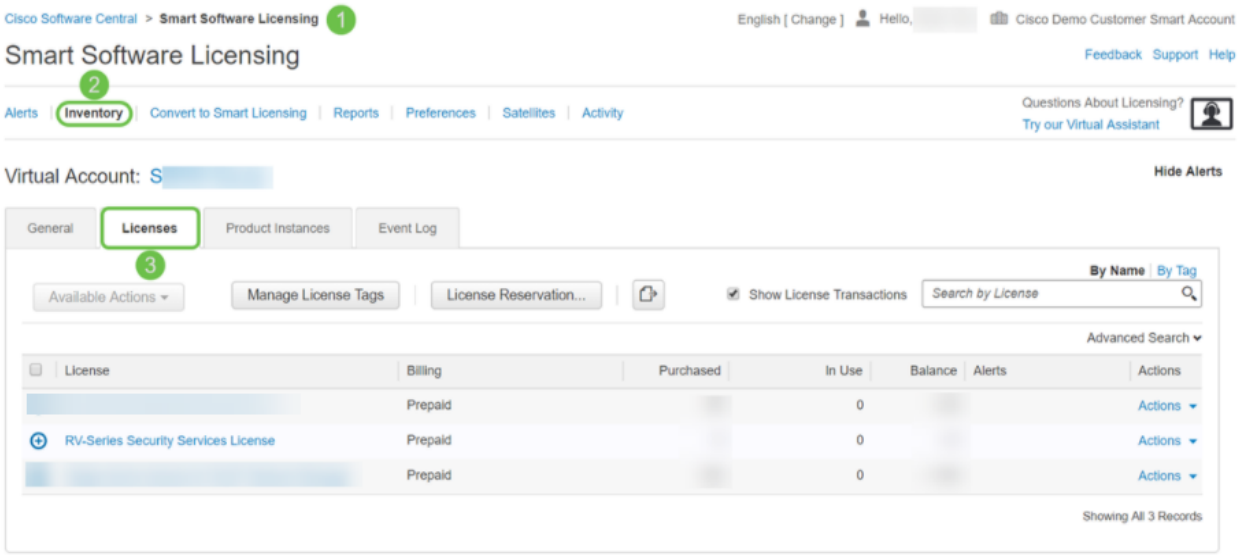
A tabela abaixo exibe o número da peça da licença.

Tipo	ID do produto	Descrição
Licença de segurança RV	LS-RV34X-SEG-1ANO=	Segurança RV: 1 ano: Filtro dinâmico da Web, visibilidade do aplicativo, identificação e estatísticas do cliente, antivírus do gateway e IPS do sistema de prevenção de intrusão.

A chave de licença não é inserida diretamente no roteador, mas será atribuída à sua Conta inteligente da Cisco depois que você solicitar a licença. O tempo que a licença leva para aparecer na sua conta depende de quando o parceiro aceita o pedido e quando o revendedor vincula as licenças à sua conta, que geralmente é de 24 a 48 horas.

Confirmar se a licença está em Smart Account

Navegue até a página da conta Smart License e clique em **Smart Software License page > Inventory > Licenses**.

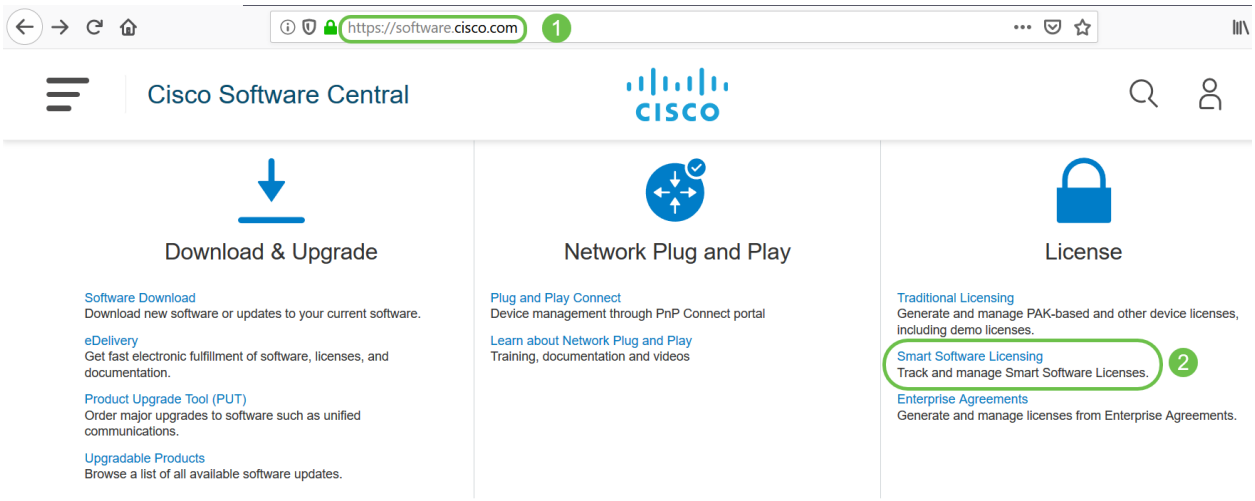


Se você não vir sua licença em sua Smart Account, entre em contato com seu parceiro da Cisco.

Configurar a licença de segurança RV no roteador RV345P Series

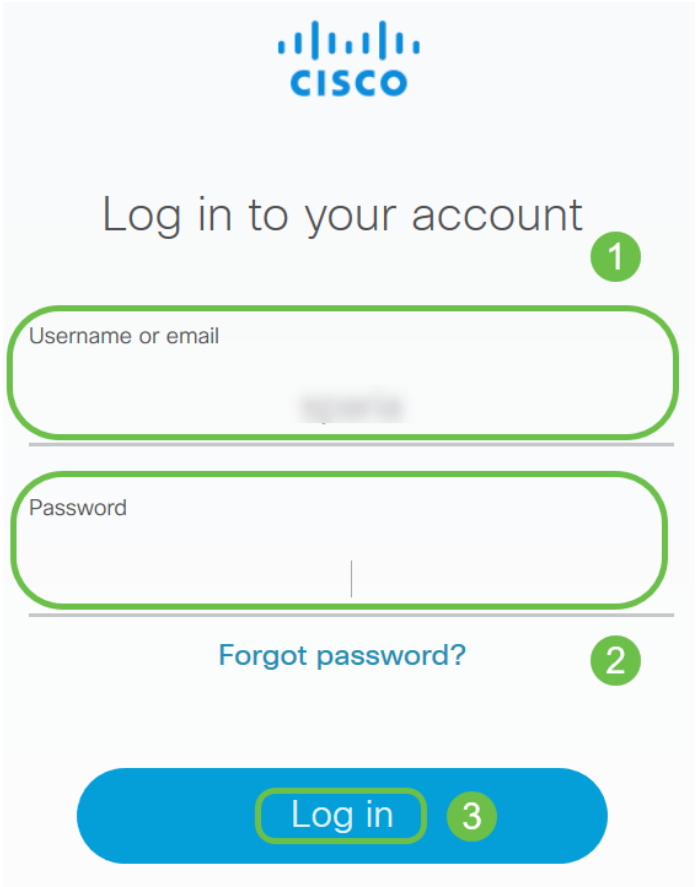
Passo 1

Acesse o software Cisco e navegue para **Smart Software Licensing**.



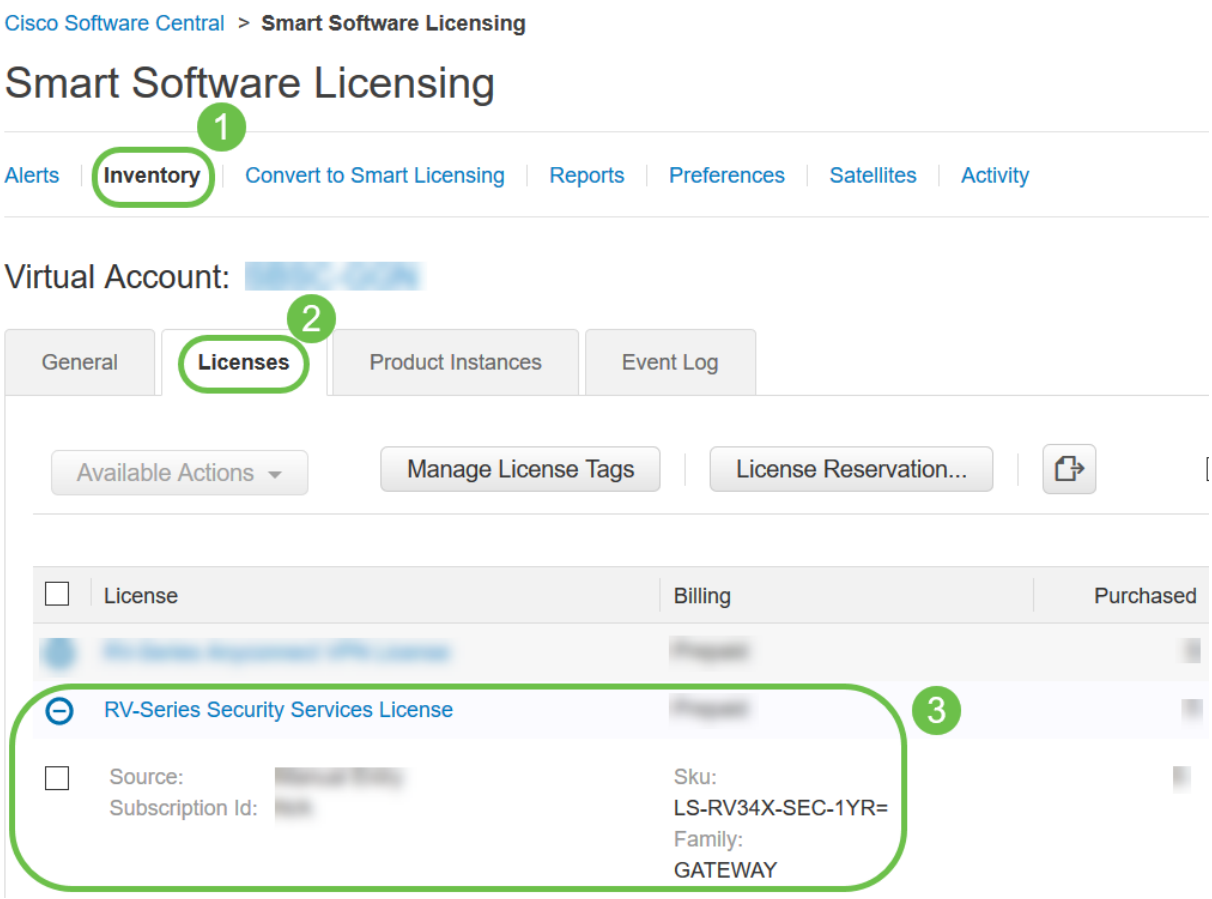
Passo 2

Digite seu *nome de usuário ou e-mail* e *senha* para fazer login em sua Smart Account. Clique em **Login**.



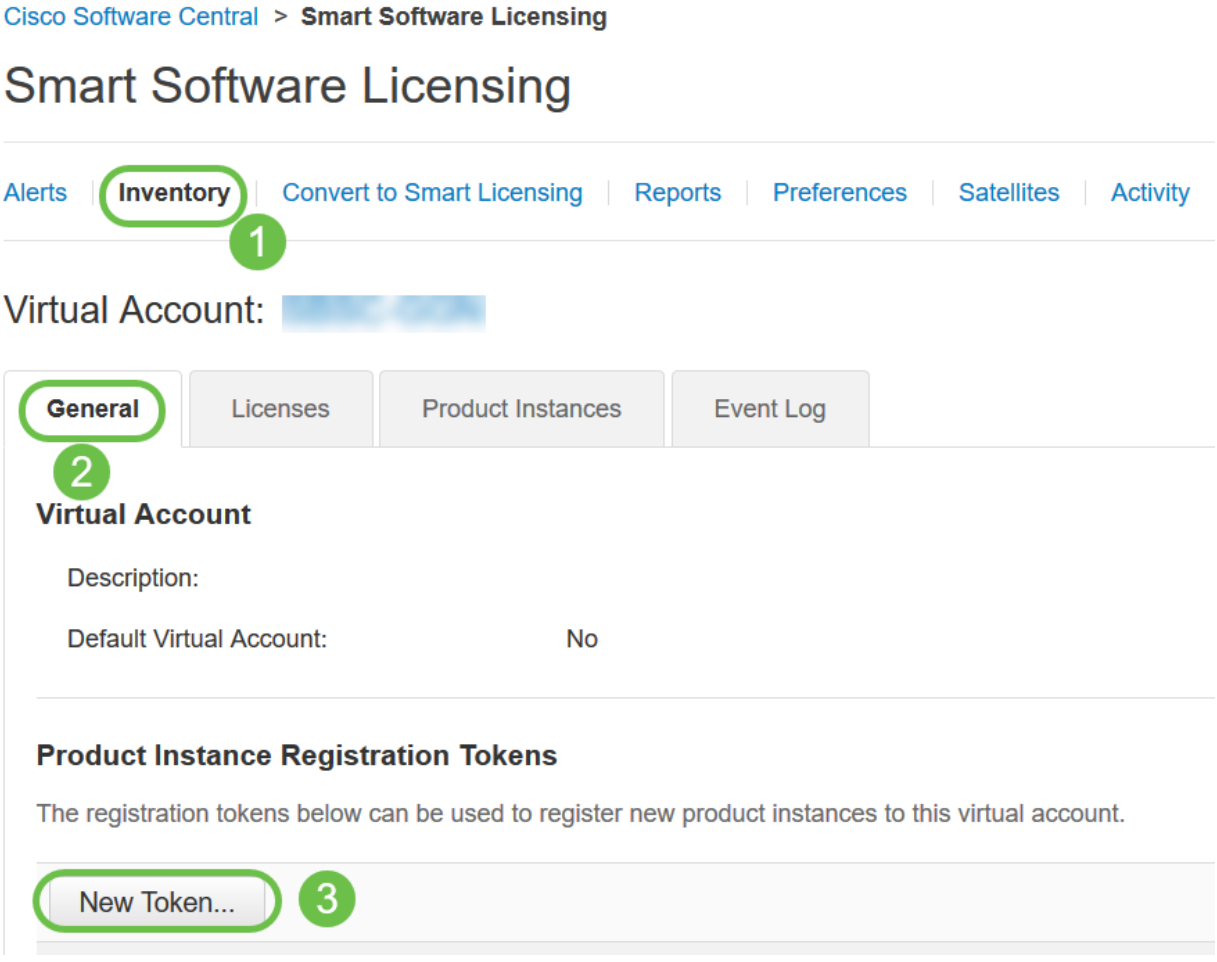
Etapa 3

Navegue até **Inventário > Licenças** e verifique se a *RV-Series Security Services License* está listada em sua Smart Account. Se você não vir a licença listada, entre em contato com seu parceiro da Cisco.



Passo 4

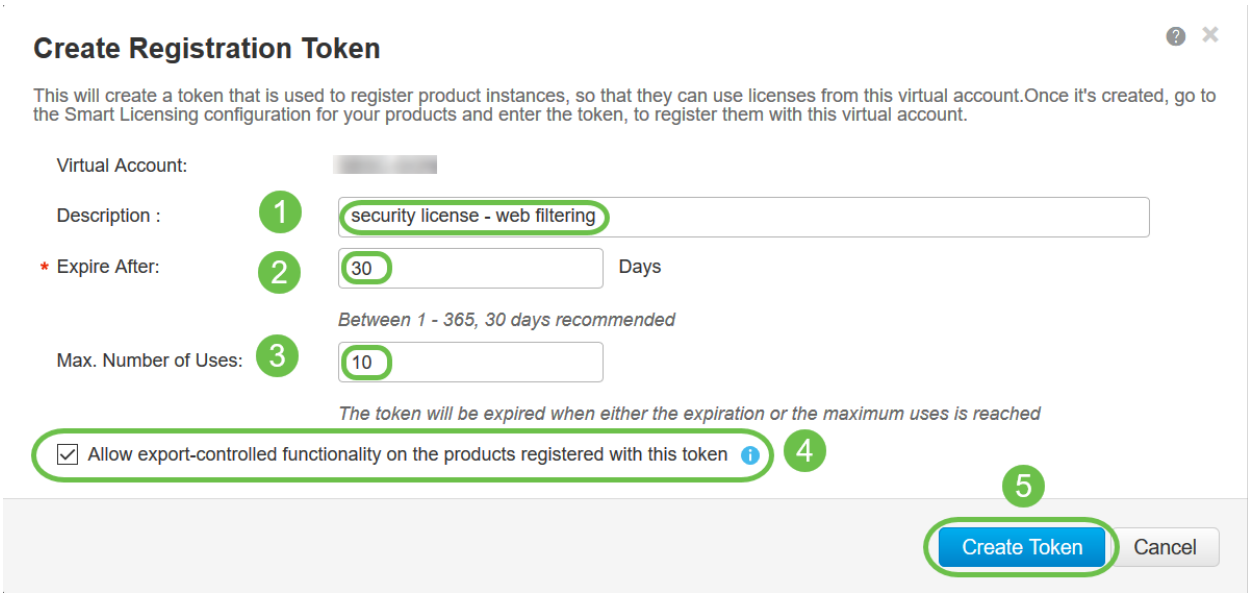
Navegue até **Inventário > Geral**. Em *Tokens de registro de instância de produto*, clique em **Novo token**.



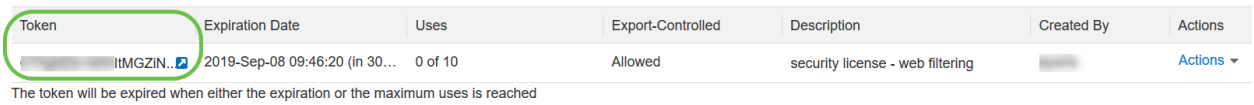
Etapa 5

Uma janela Create Registration Token (Criar token de registro) será exibida. A área *Virtual Account* exibe a Virtual Account na qual o token de registro será criado. Na página *Create Registration Token*, faça o seguinte:

- No campo Descrição, insira uma descrição exclusiva para o token. Neste exemplo, licença de segurança - a filtragem da Web é inserida.
- No campo Expirar após, insira um valor entre 1 e 365 dias. A Cisco recomenda o valor de 30 dias para este campo; entretanto, você pode editar o valor para atender às suas necessidades.
- No máximo. Número de Usos insira um valor para definir o número de vezes que você deseja usar esse token. O token expirará quando a quantidade de dias ou o número máximo de usos for atingido.
- Marque a caixa de seleção Permitir funcionalidade controlada por exportação nos produtos registrados com este token para ativar a funcionalidade controlada por exportação para tokens de uma instância de produto na sua conta virtual. Desmarque a caixa de seleção se não quiser permitir que a funcionalidade controlada por exportação seja disponibilizada para uso com este token. Use esta opção somente se estiver em conformidade com a funcionalidade controlada por exportação. Alguns recursos controlados por exportação são restritos pelo Departamento de Comércio dos Estados Unidos. Esses recursos são restritos para produtos registrados usando este token quando você desmarca a caixa de seleção. Quaisquer violações são sujeitas a sanções e encargos administrativos.
- Clique em **Create Token** para gerar o token.



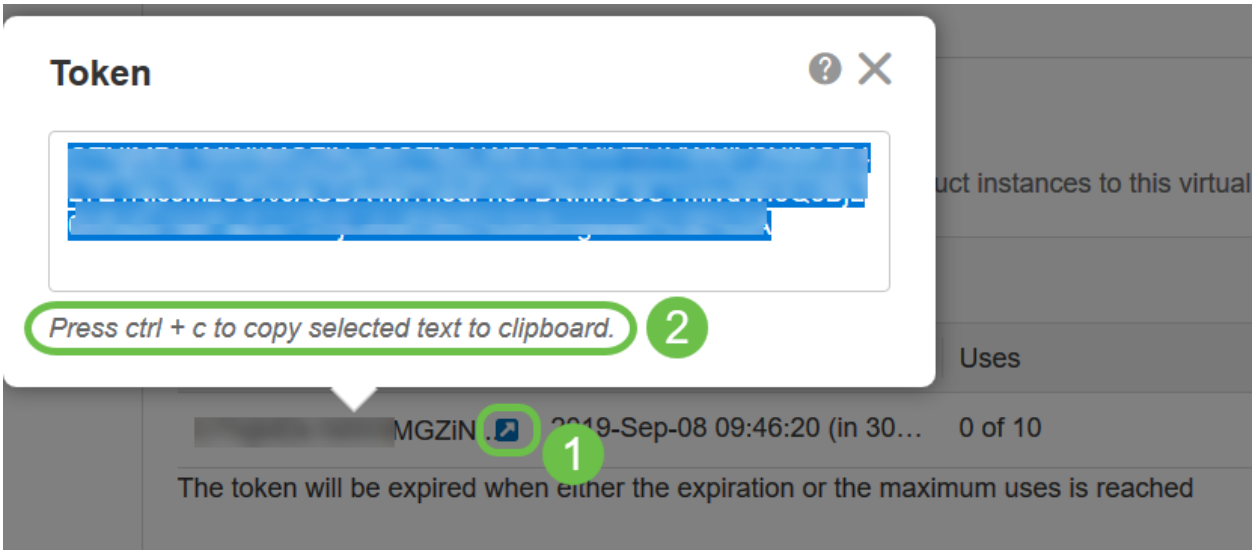
Agora você gerou com êxito um token de registro de instância de produto.



Etapa 6

Clique no **ícone de seta** na coluna *Token* para copiar o token para a área de

transferência, pressione **ctrl + c** no teclado.

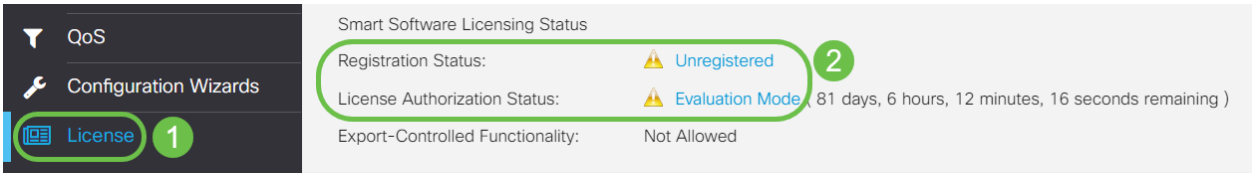


Etapa 7 (opcional)

Clique no menu suspenso **Ações**, escolha **Copiar** para copiar o token para a área de transferência ou **Download...** para baixar uma cópia de arquivo de texto do token do qual você pode copiar.

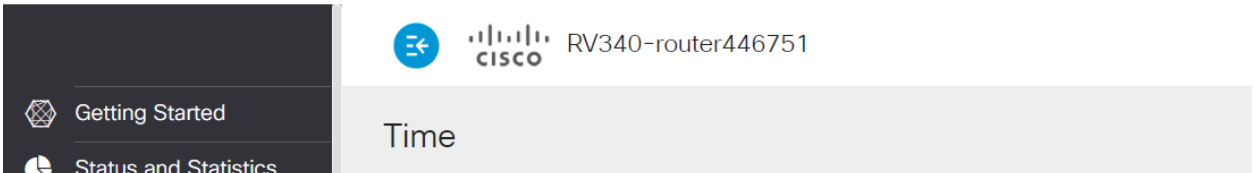
Passo 8

Navegue até Licença e verifique se o *Status do registro* é exibido como *Não registrado* e *Status da autorização de licença* é exibido como *Modo de avaliação*.



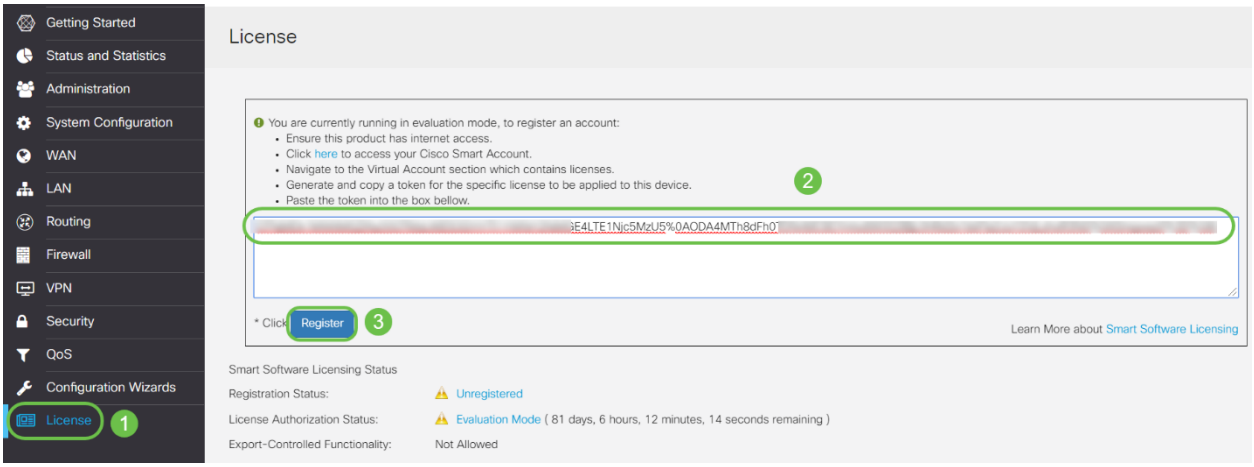
Passo 9

Navegue até **System Configuration > Time** e verifique se *Current Date and Time* and *Time Zone* estão refletindo corretamente de acordo com o seu fuso horário.



Passo 10

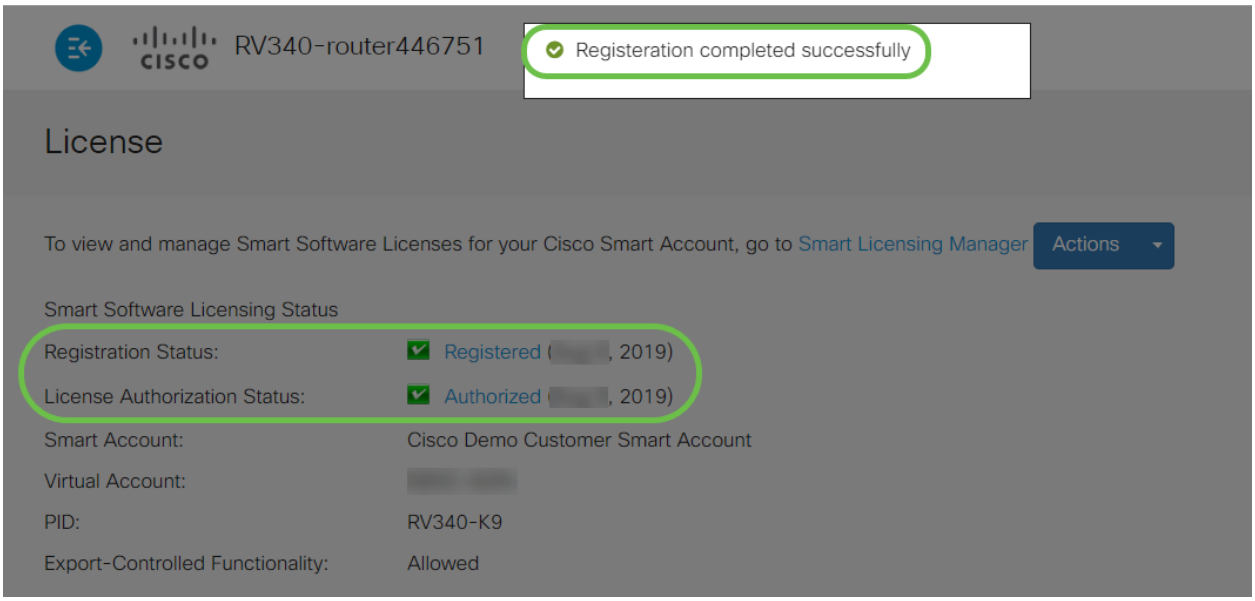
Navegue até **Licença**. Cole o token copiado na etapa 6 na caixa de texto na guia *Licença* selecionando **ctrl + v** no teclado. Clique em **Registrar**.



O registro pode levar alguns minutos. Não saia da página quando o roteador tentar entrar em contato com o servidor de licenças.

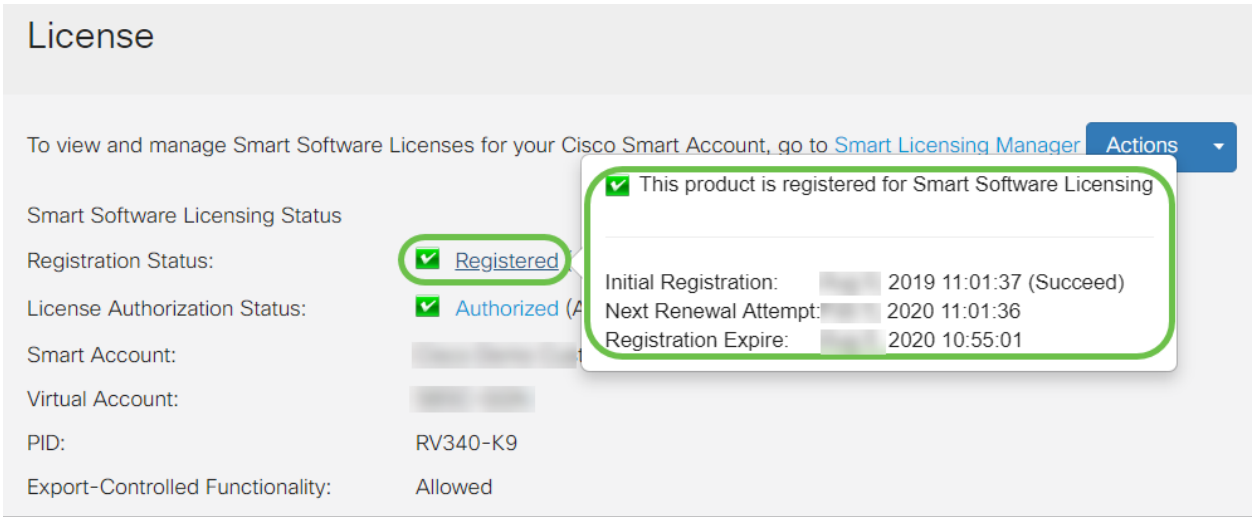
Passo 11

Agora você deve ter registrado e autorizado com êxito seu roteador RV345P Series com uma Smart License. Você receberá uma notificação na tela *Registro concluído com êxito*. Além disso, você poderá ver que o *Status do registro* é exibido como *Registrado* e que o *Status da autorização de licença* é mostrado como *Autorizado*.



Etapa 12 (Opcional)

Para ver mais detalhes sobre o *Status do registro* da licença, passe o ponteiro sobre o status *Registrado*. Uma mensagem de diálogo é exibida com as seguintes informações:

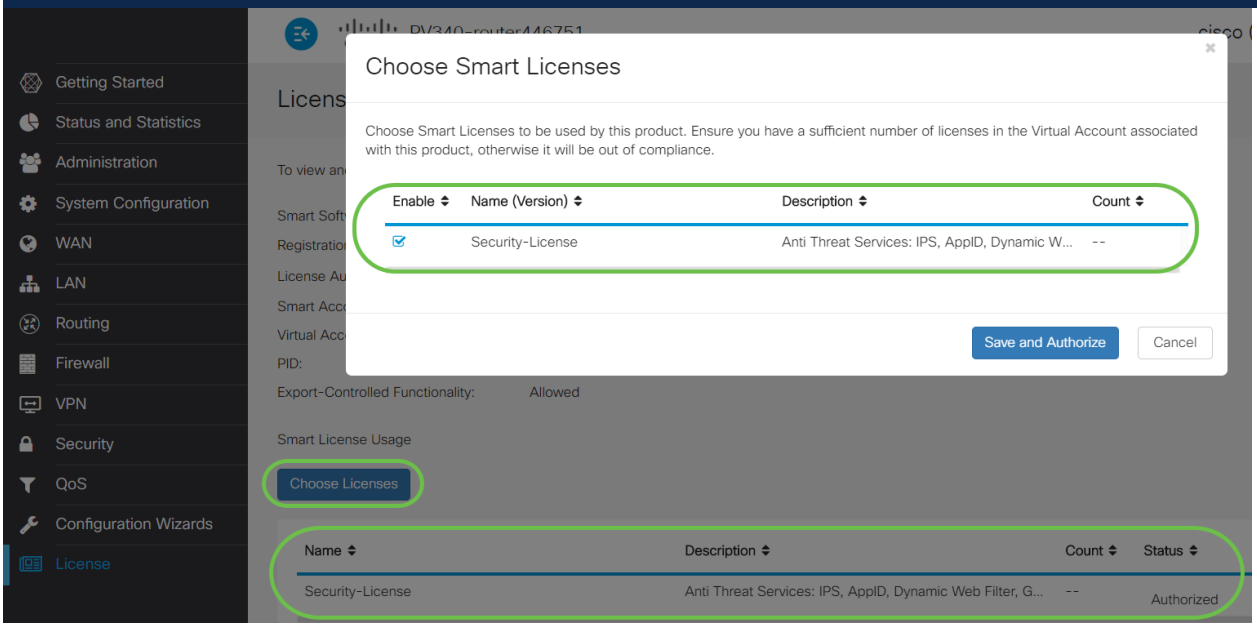


- Registro inicial — Essa área indica a data e a hora de registro da licença.
- Próxima tentativa de renovação — Essa área indica a data e a hora em que o roteador tentará renovar a licença.
- Registration Expire — Essa área indica a data e a hora em que o registro expira.

Passo 13

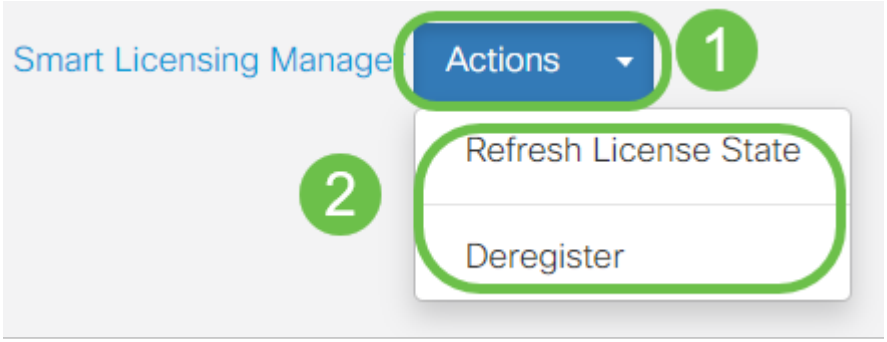
Na página *Licença*, verifique se o status *Security-License* está mostrando *Authorized (Autorizado)*. Você também pode clicar no botão **Escolher licença** para verificar se a *licença de segurança* está ativada.

Se tiver problemas nessa etapa, talvez seja necessário reinicializar o roteador.



Etapa 14 (Opcional)

Para *Atualizar o Estado da Licença* ou *Cancelar o registro* da licença do roteador, clique no menu suspenso **Ações do** *Smart Licensing Manager* e selecione um item de ação.



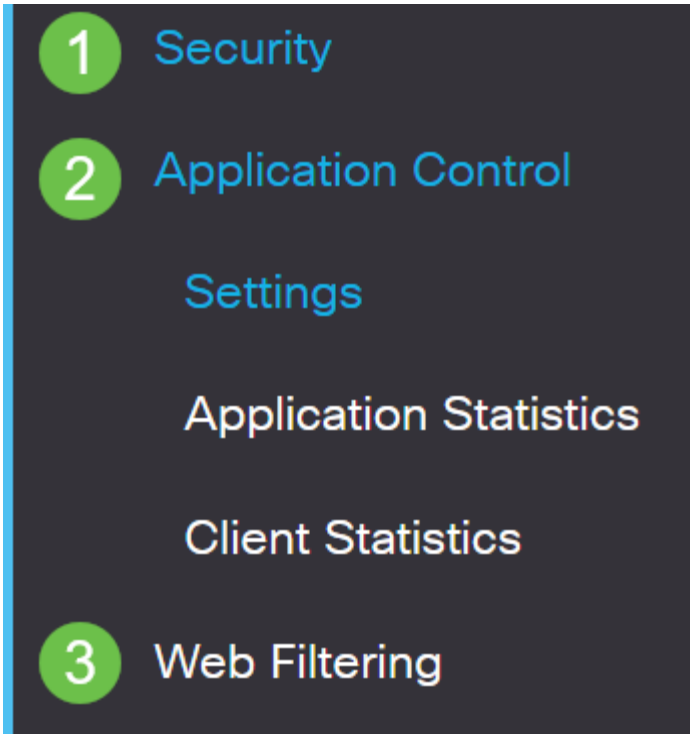
Agora que você tem sua licença no roteador, você precisa concluir as etapas na próxima seção.

Filtragem da Web no roteador RV345P

Você tem 90 dias após a ativação para usar a filtragem da Web sem nenhum custo. Após a avaliação gratuita, se desejar continuar usando esse recurso, você precisará comprar uma licença. Clique para voltar para essa seção.

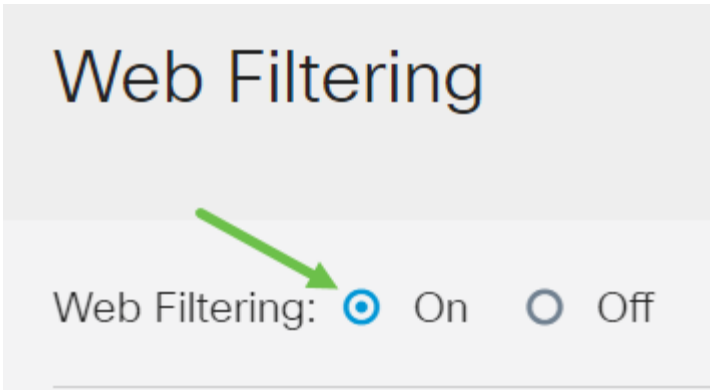
Passo 1

Efetue login no utilitário baseado na Web e escolha **Security > Application Control > Web Filtering (Segurança > Controle de aplicativos > Filtragem da Web)**.



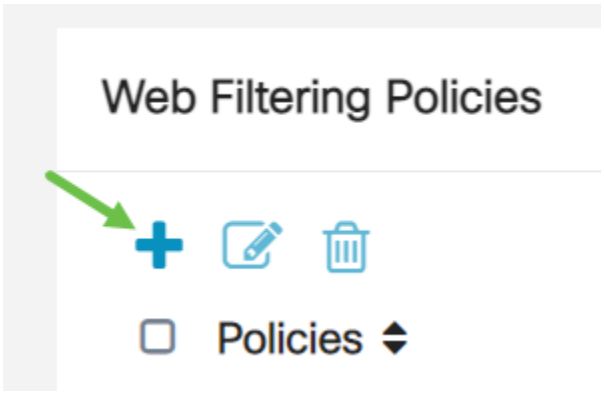
Passo 2

Selecione o botão de opção **On (Ativado)**.



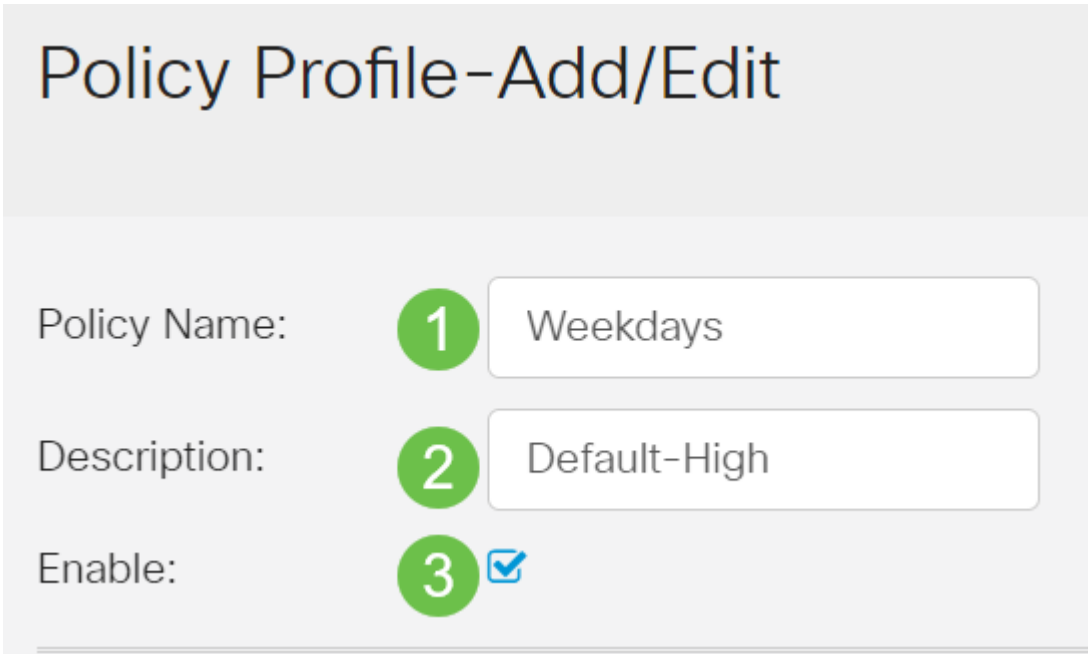
Etapa 3

Clique no **ícone Adicionar**.



Passo 4

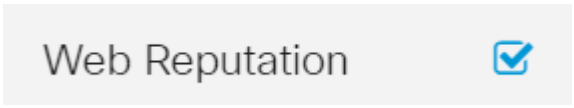
Insira um *Nome da diretiva*, *Descrição* e a caixa de seleção *Habilitar*.



Se a Filtragem de conteúdo estiver habilitada em seu roteador, uma notificação aparecerá para informá-lo de que a Filtragem de conteúdo foi desativada e que os dois recursos não podem ser ativados simultaneamente. Clique em **Apply** para continuar com a configuração.

Etapa 5

Marque a caixa de seleção Web Reputation para ativar a filtragem com base em um índice de reputação da Web.

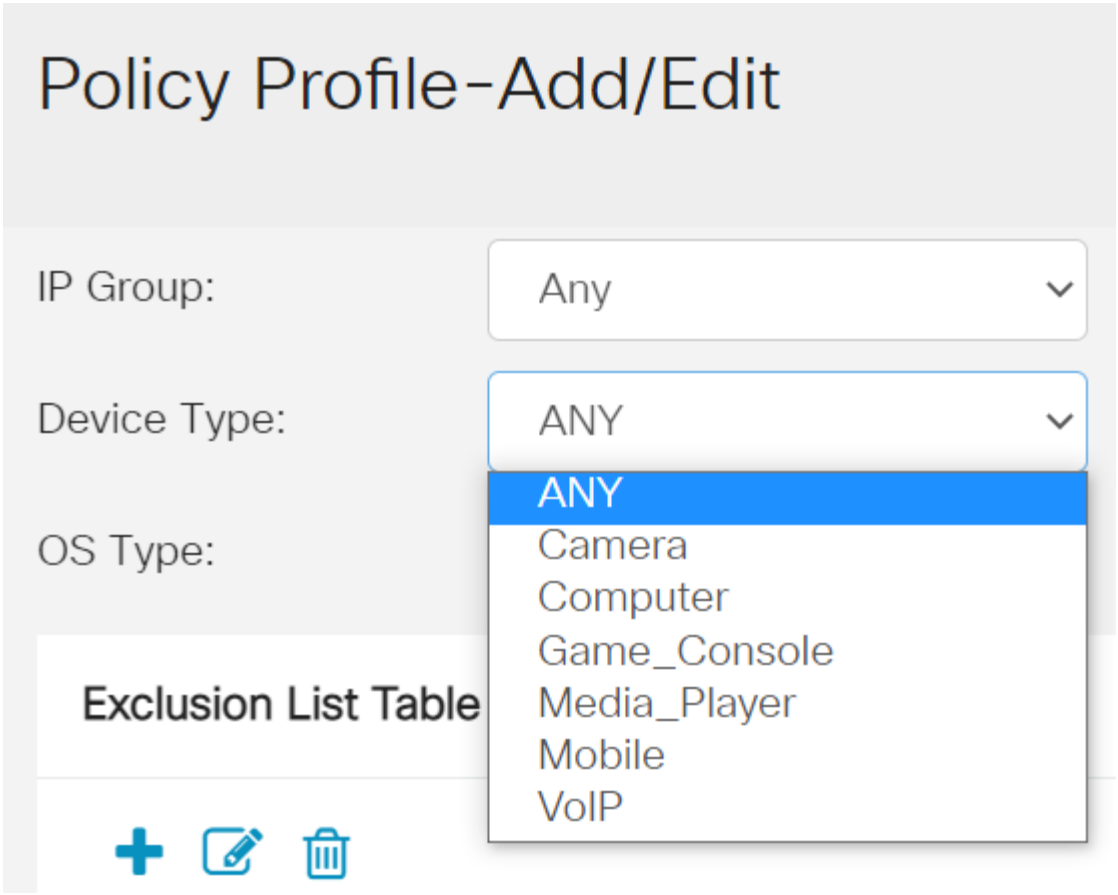


O conteúdo será filtrado de acordo com a notoriedade de um site ou URL baseado em um índice de reputação da Web. Se a pontuação cair abaixo de 40, o site será bloqueado. Para ler mais sobre a tecnologia de reputação da Web, clique aqui para obter mais detalhes.

Etapa 6

Na lista suspensa *Tipo de dispositivo*, selecione a origem/destino dos pacotes a serem filtrados. Apenas uma opção pode ser escolhida de cada vez. As opções são:

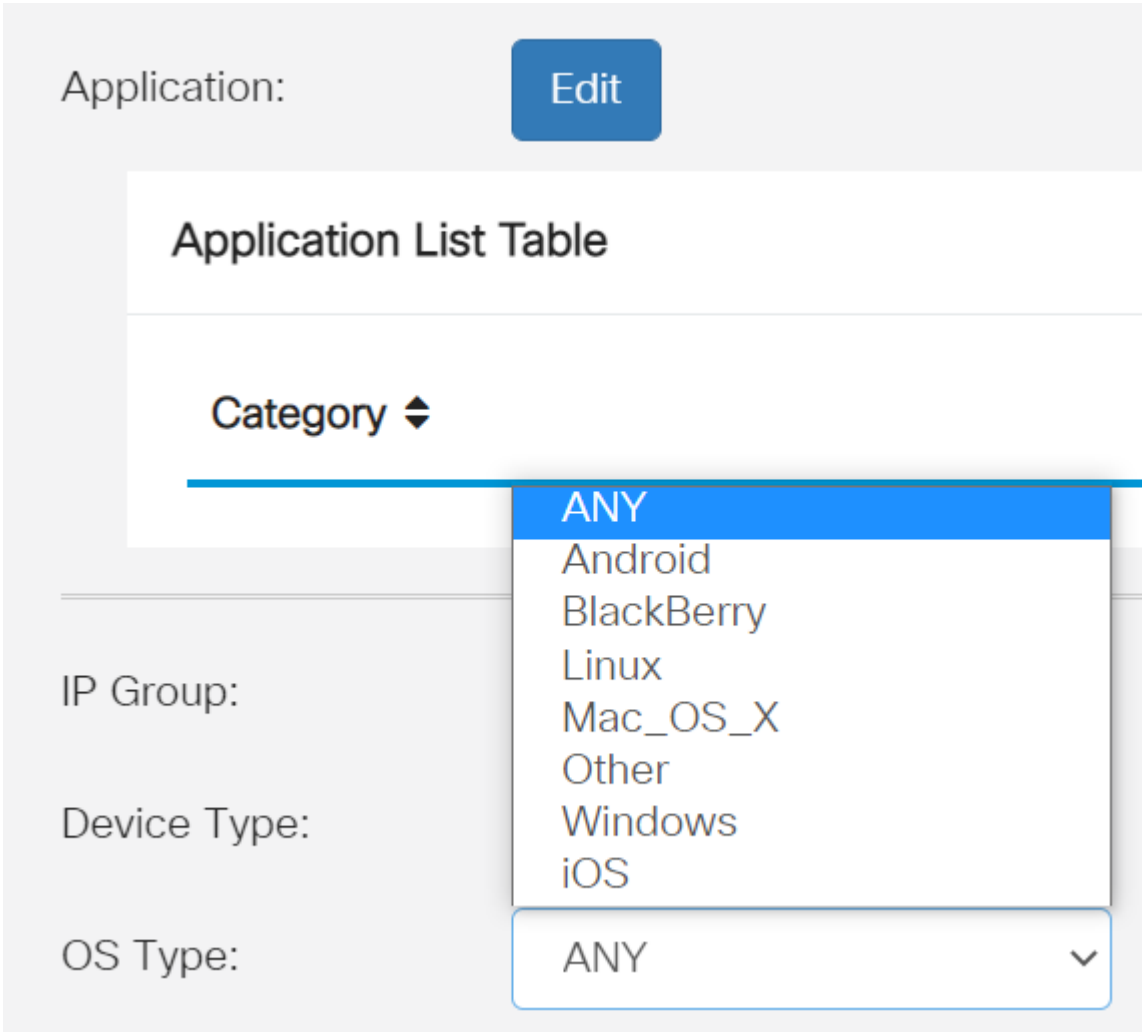
- ANY — Escolha esta opção para aplicar a política a qualquer dispositivo.
- Câmera — Escolha essa opção para aplicar a política às câmeras (como câmeras de segurança IP).
- Computador — Escolha esta opção para aplicar a política aos computadores.
- Game_Console — Escolha esta opção para aplicar a política aos consoles de jogos.
- Media_Player — Escolha esta opção para aplicar a política aos Media Players.
- Móvel — Escolha esta opção para aplicar a política aos dispositivos móveis.
- VoIP — Escolha esta opção para aplicar a política aos dispositivos Voice over Internet Protocol .



Etapa 7

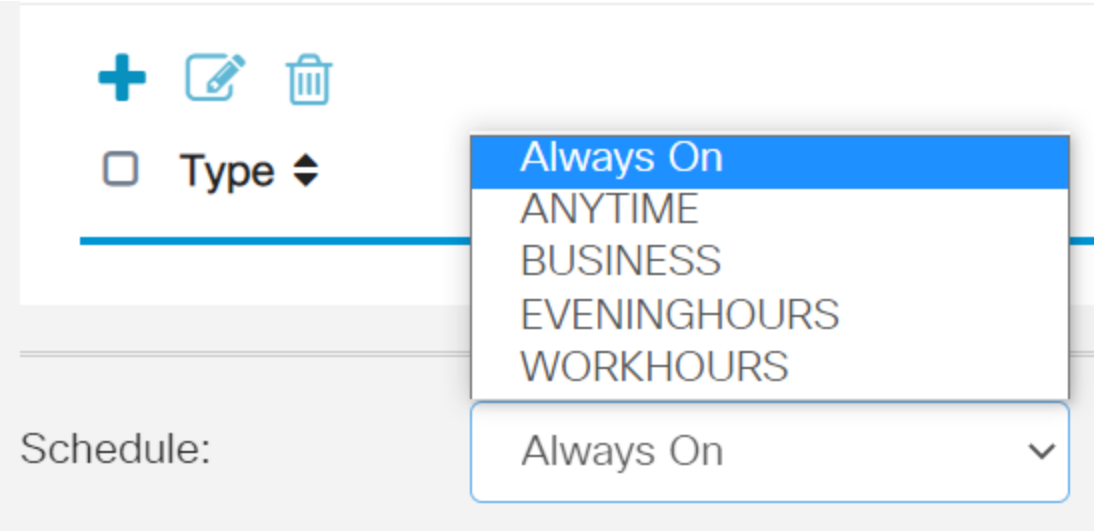
Na lista suspensa *Tipo de SO*, escolha um sistema operacional (SO) ao qual a política deve ser aplicável. Apenas uma opção pode ser escolhida de cada vez. As opções são:

- ANY — Aplica a política a qualquer tipo de SO. Esse é o padrão.
- Android — Aplica a política somente ao sistema operacional Android.
- BlackBerry — Aplica a política somente ao Blackberry OS.
- Linux — Aplica a política somente ao sistema operacional Linux.
- Mac_OS_X — Aplica a política somente ao Mac OS.
- Outro — Aplica a política a um SO que não está listado.
- Windows — Aplica a política ao sistema operacional Windows.
- iOS — Aplica a política somente ao iOS OS.



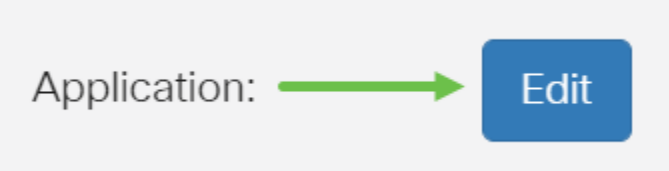
Passo 8

Role para baixo até a seção *Agendar* e selecione a opção mais adequada às suas necessidades.



Passo 9

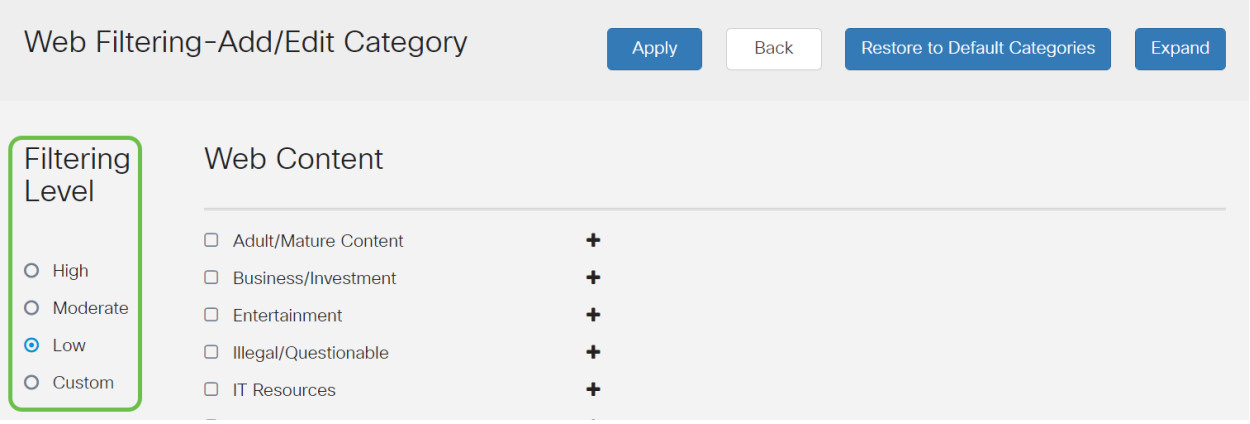
Clique no **ícone de edição**.



Passo 10

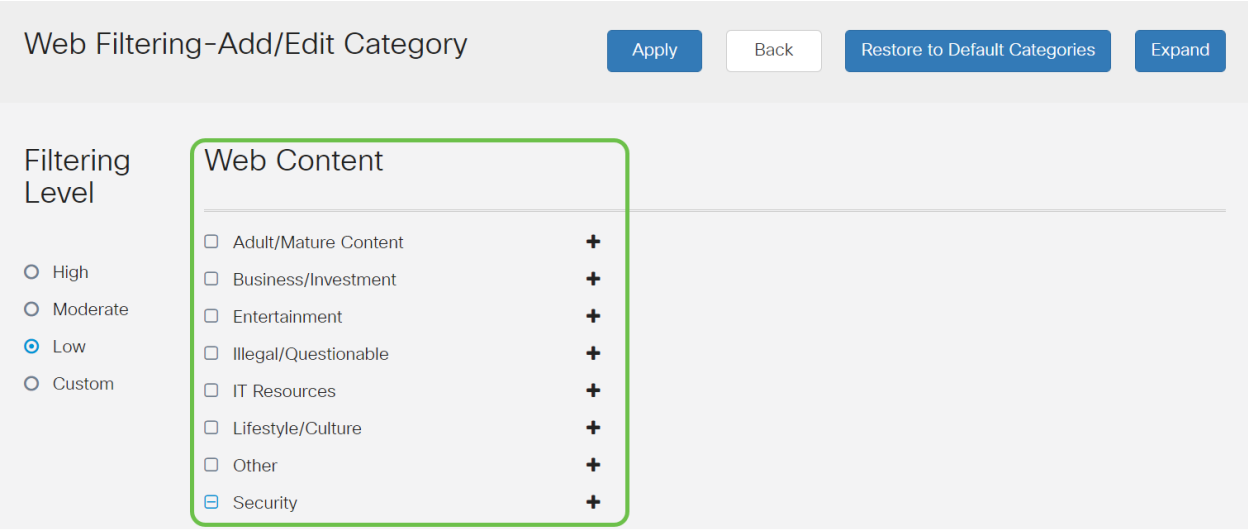
Na coluna Nível de filtragem, clique em um botão de opção para definir rapidamente a extensão de filtragem que melhor se adapta às políticas de rede. As opções são Alto, Moderado, Baixo e Personalizado. Clique em qualquer um dos níveis de filtragem abaixo para saber as subcategorias predefinidas específicas filtradas para cada uma de suas categorias de conteúdo da Web habilitadas. Os filtros pré-definidos não podem ser alterados mais e estão esmaecidos.

- Low — Esta é a opção padrão. A segurança está ativada com esta opção.
- Moderado — Conteúdo adulto/maduro, ilegal/questionável e segurança são ativados com essa opção.
- Alto — Conteúdo para adultos/maduros, Negócios/Investimentos, Ilegal/Questionável, Recursos de TI e Segurança são ativados com essa opção.
- Personalizado — Nenhum padrão é definido para permitir filtros definidos pelo usuário.



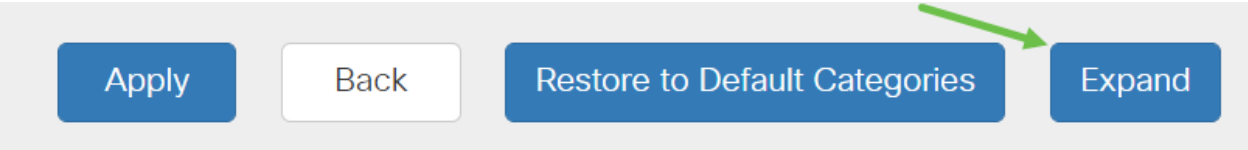
Passo 11

Insira o conteúdo da Web que deseja filtrar. Clique no **ícone de mais** se quiser mais detalhes em uma seção.



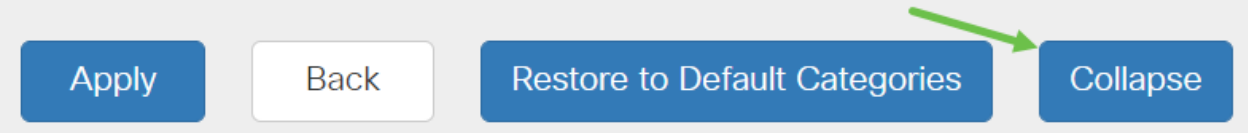
Etapa 12 (Opcional)

Para visualizar todas as subcategorias e descrições de Conteúdo da Web, clique no botão **Expandir**.



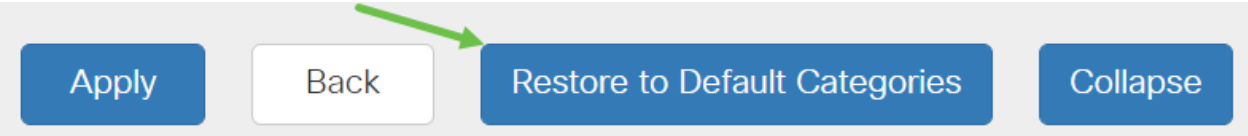
Etapa 13 (Opcional)

Clique em **Recolher** para recolher as subcategorias e descrições.



Etapa 14 (Opcional)

Para retornar às categorias padrão, clique em **Restaurar para categorias padrão**.



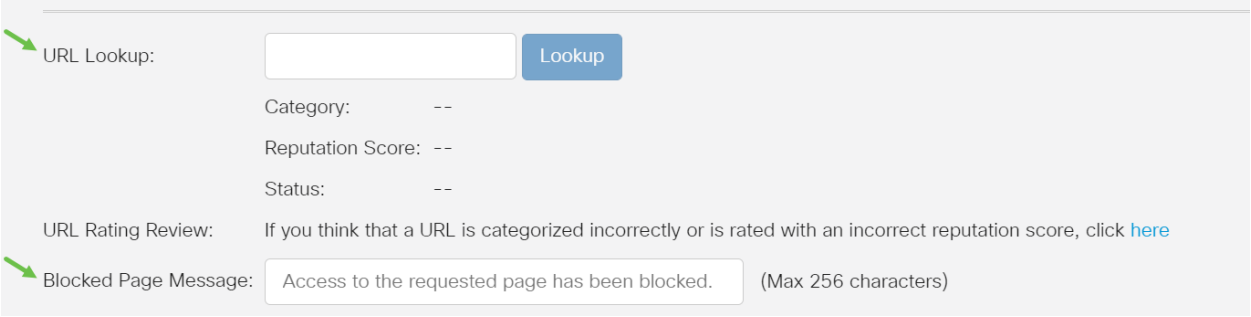
Etapa 15

Clique em **Apply** para salvar a configuração e retornar à página Filter (Filtro) para continuar a configuração.

Na Tabela Lista de aplicativos, as subcategorias correspondentes baseadas no nível de filtragem escolhido preencherão a tabela.

Etapa 16 (Opcional)

Outras opções incluem a Pesquisa de URL e a mensagem que mostra quando uma página solicitada foi bloqueada.



Etapa 17 (Opcional)

Clique em Apply.

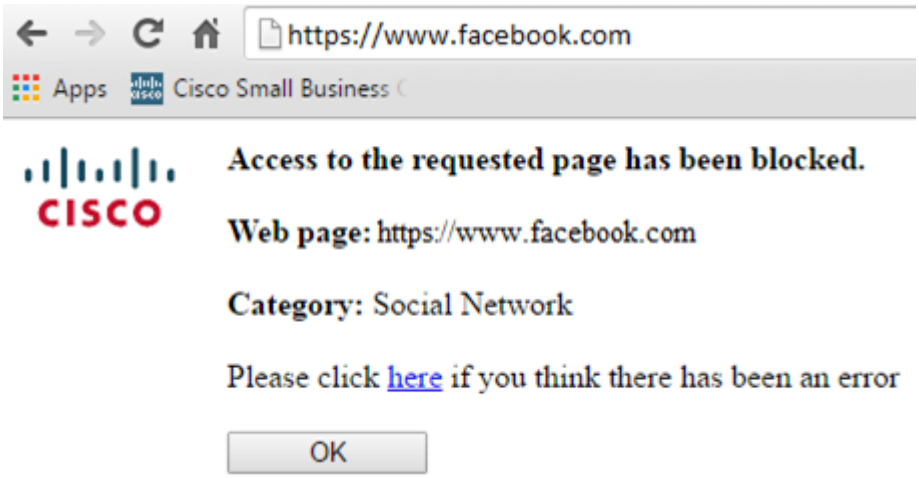
Etapa 18

Para salvar a configuração permanentemente, vá para a página *Copiar/salvar configuração* ou clique no **ícone salvar** na parte superior da página.

Etapa 19 (Opcional)

Para verificar se um site ou URL foi filtrado ou bloqueado, inicie um navegador da Web ou abra uma nova guia no navegador. Insira o nome de domínio que você tem bloqueado ou que foi filtrado para ser bloqueado ou negado.

Neste exemplo, usamos www.facebook.com.



Agora você deve ter configurado com êxito a filtragem da Web no roteador RV345P. Como você está usando a Licença de segurança RV para filtragem da Web, provavelmente não precisa do Umbrella. Se você também quiser o Umbrella, clique aqui. Se você tiver segurança suficiente, clique para ir para a próxima seção.

Troubleshooting

Se você adquiriu uma licença, mas ela não aparece em sua conta virtual, você tem duas opções:

1. Acompanhe o revendedor para solicitar a transferência.
2. Entre em contato conosco e entraremos em contato com o revendedor.

Idealmente, você também não precisaria fazer isso, mas se você chegar a essa encruzilhada, ficaremos felizes em ajudar! Para tornar o processo o mais rápido possível, você precisará das credenciais na tabela acima, bem como das descritas abaixo.

Informações necessárias	Localização das informações
Fatura da licença	Isso deve ser enviado por e-mail a você após concluir a compra das licenças.
Número do pedido de vendas da Cisco	Talvez você precise voltar para o revendedor para obter isso.
Captura de tela da sua página de licença da Smart Account	Tirar uma captura de tela captura o conteúdo da tela para compartilhamento com nossa equipe. Se você não está familiarizado com capturas de tela, use os métodos abaixo.

Capturas de tela

Quando você tiver um token ou estiver solucionando problemas, é recomendável tirar uma captura de tela para capturar o conteúdo da tela.

Dadas as diferenças no procedimento necessário para capturar uma captura de tela, consulte abaixo os links específicos ao seu sistema operacional.

- Windows
- MAC
- iPhone/iPad
- Android

Licença para filiais de RV Umbrella (opcional)

O Umbrella é uma plataforma de segurança em nuvem simples, mas muito eficaz da Cisco.

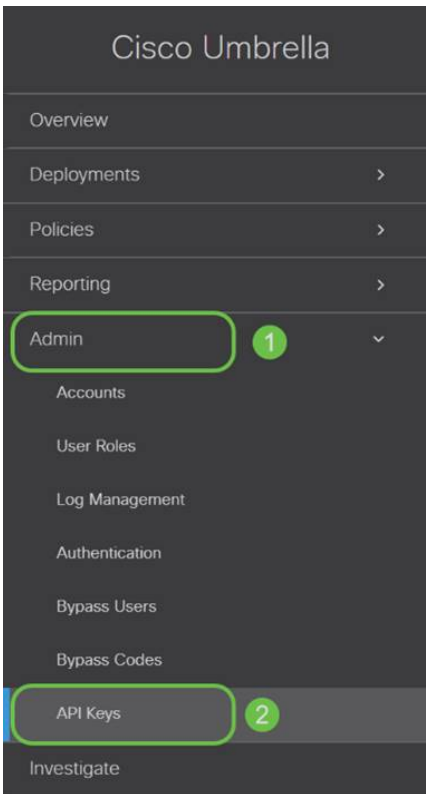
O Umbrella opera na nuvem e executa muitos serviços relacionados à segurança. Da ameaça emergente à investigação pós-evento. O Umbrella descobre e evita ataques em todas as portas e protocolos.

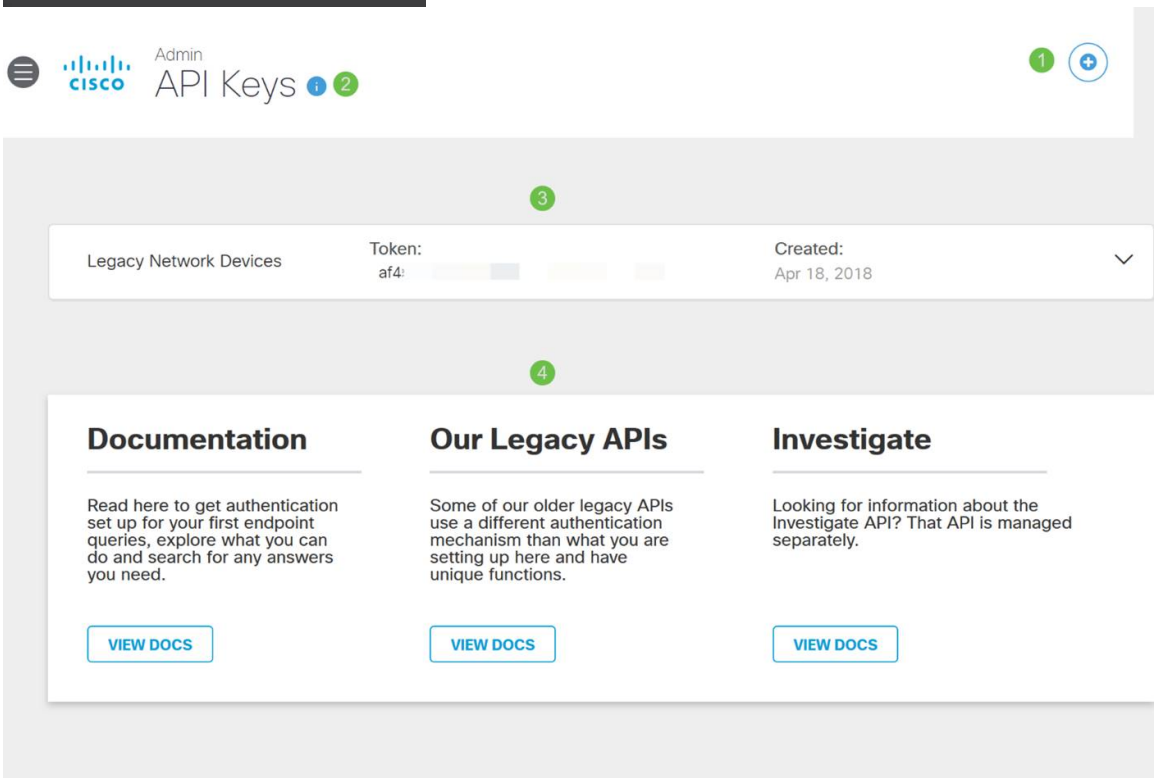
O Umbrella usa o DNS como seu principal vetor de defesa. Quando os usuários inserem um URL na barra do navegador e pressionam *Enter*, o Umbrella participa da transferência. Essa URL passa para o resolvedor DNS do Umbrella e, se um aviso de segurança se associar ao domínio, a solicitação é bloqueada. Essa telemetria transfere dados e é analisada em microssegundos, adicionando quase nenhuma latência. Os dados de telemetria usam logs e instrumentos para rastrear bilhões de solicitações DNS em todo o mundo. Quando esses dados são difundidos, correlacioná-los em todo o mundo permite uma resposta rápida aos ataques à medida que eles começam. Consulte a política de privacidade da Cisco aqui para obter mais informações: política completa, versão resumida. Pense nos dados de telemetria como dados derivados de ferramentas e registros.

Visite o Cisco Umbrella para saber mais e criar uma conta. Se tiver problemas, consulte aqui a documentação e aqui para ver as opções de suporte do Umbrella.

Passo 1

Depois de fazer login em sua Conta Umbrella, na tela *Dashboard,* clique em **Admin** > **API Keys**.



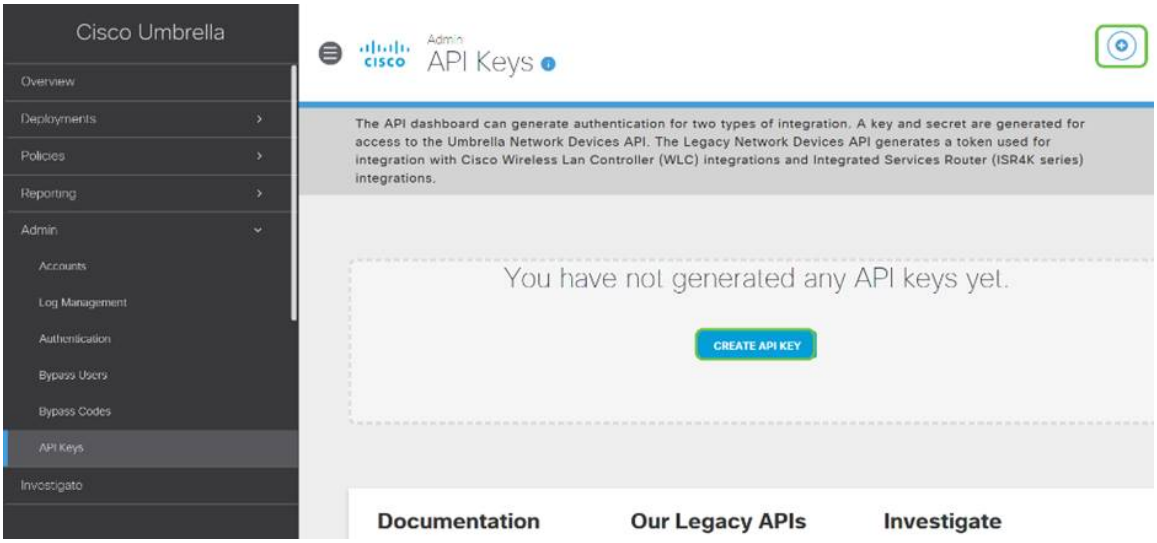


Anatomia da tela de chaves API (com chave API pré-existente)

1. Add API Key (Adicionar chave de API) - Inicia a criação de uma nova chave para uso com a API Umbrella.
2. Informações adicionais - desliza para baixo/para cima com um explicador para esta tela.
3. Token Well - Contém todas as chaves e tokens criados por esta conta. (Preenche uma vez que uma chave foi criada)
4. Documentos de suporte - Links para a documentação no site Umbrella referente aos tópicos em cada seção.

Passo 2

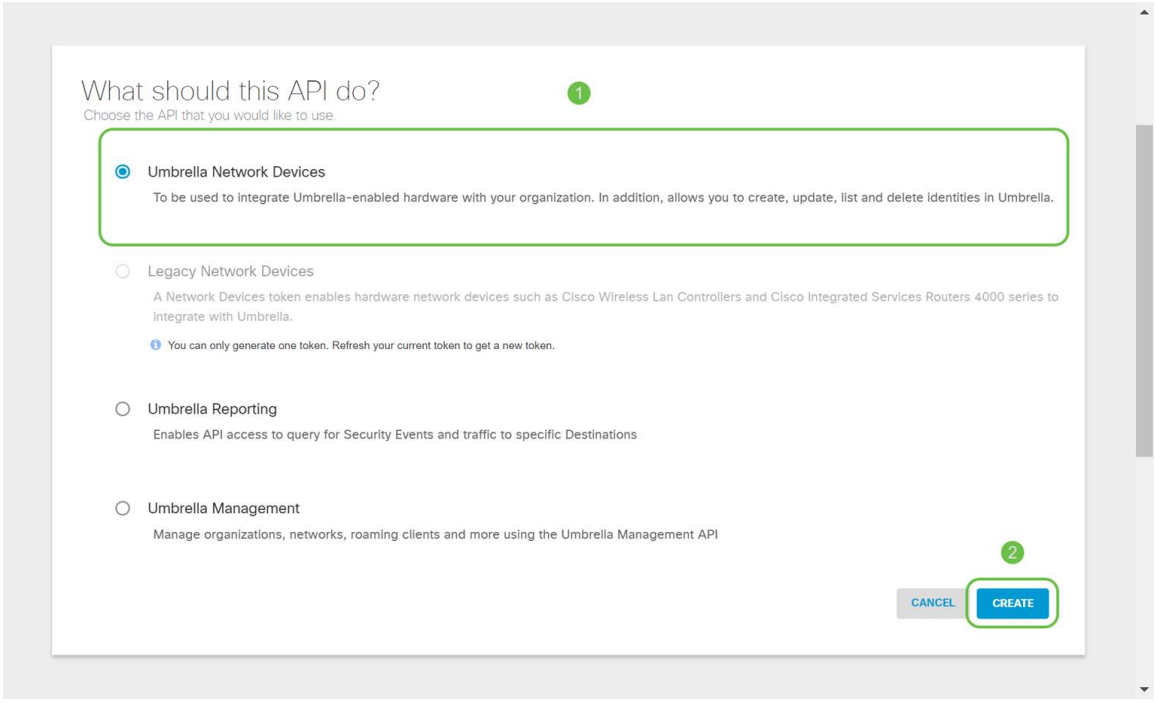
Clique no botão **Add API Key** (Adicionar chave de API) no canto superior direito ou clique no botão **Create API Key (Criar chave de API)**. Ambos funcionam da mesma forma.



A captura de tela acima seria semelhante ao que você veria abrindo este menu pela primeira vez.

Etapa 3

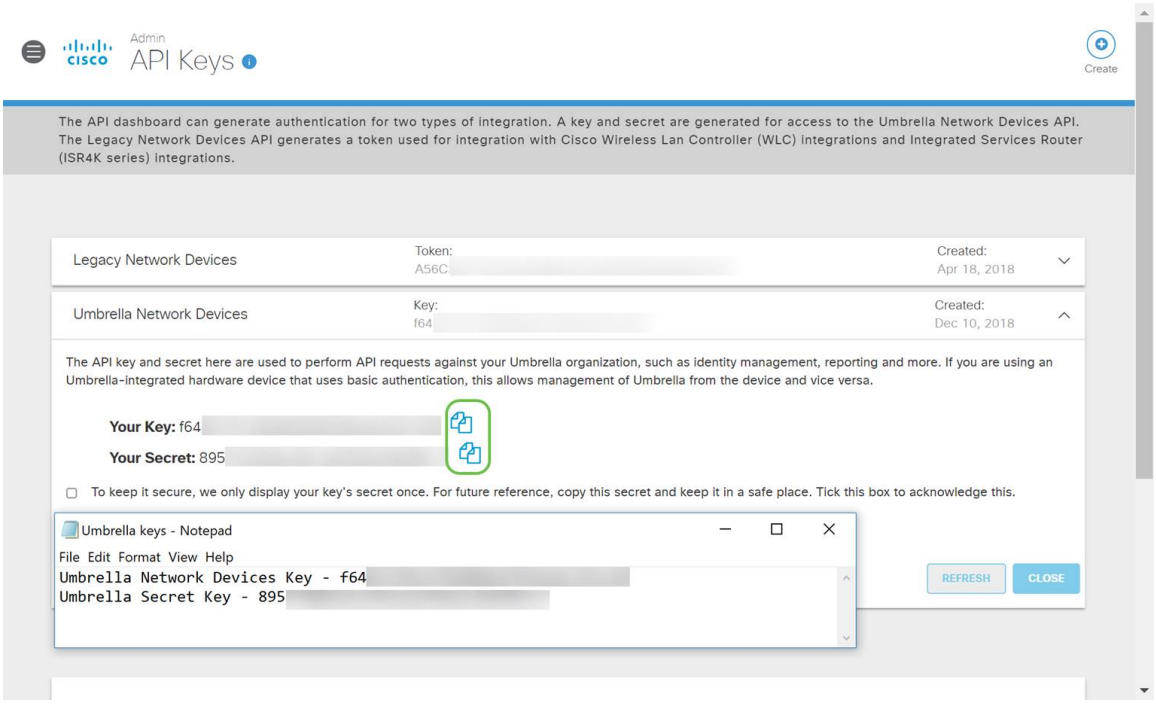
Selecione **Umbrella Network Devices** e clique no botão **Create**.



Passo 4

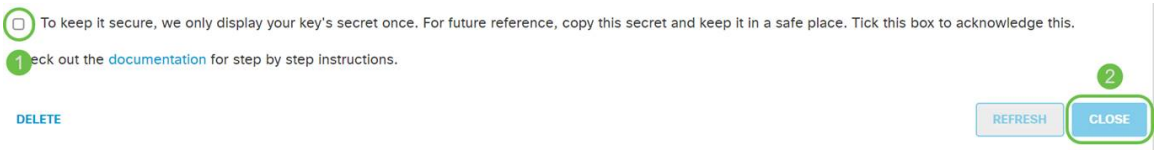
Abra um editor de texto, como o bloco de notas, e clique no **ícone de cópia** à direita da API e da *chave secreta* API, uma notificação pop-up confirmará que a chave foi

copiada para a área de transferência. Cole, um de cada vez, sua chave secreta e API no documento, rotulando-os para referência futura. Nesse caso, sua etiqueta é "Chave dos dispositivos de rede Umbrella". Em seguida, salve o arquivo de texto em um local seguro, fácil de acessar posteriormente.



Etapa 5

Depois de copiar a chave e a chave secreta em um local seguro, na *tela da API Umbrella*, clique na **caixa de seleção** para confirmar a confirmação da exibição temporária da chave secreta e clique no botão **Fechar**.



Se você perder ou excluir acidentalmente a chave secreta, não há nenhuma função ou número de suporte para ligar para recuperar essa chave. Se perdido, você precisará excluir a chave e reautorizar a nova chave API com cada dispositivo que deseja proteger com o Umbrella.

Configurando o Umbrella no RV345P

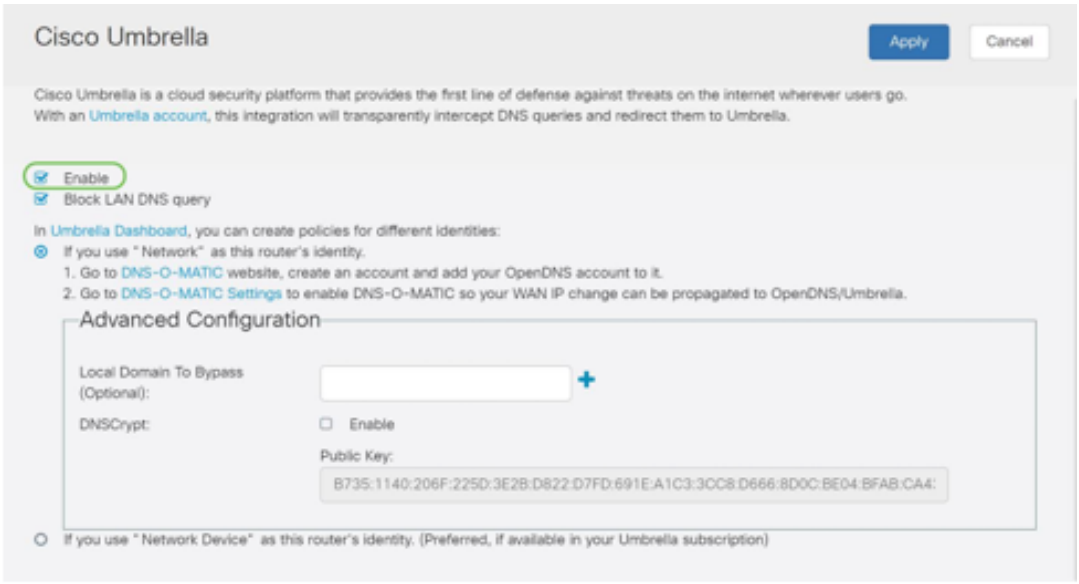
Agora que criamos chaves de API no Umbrella, você pode pegar essas chaves e instalá-las no RV345P.

Passo 1

Depois de fazer login no roteador RV345P, clique em **Security > Umbrella** no menu da barra lateral.

Passo 2

A tela da API Umbrella tem várias opções. Comece a ativar o Umbrella clicando na caixa de seleção **Enable (Habilitar)**.

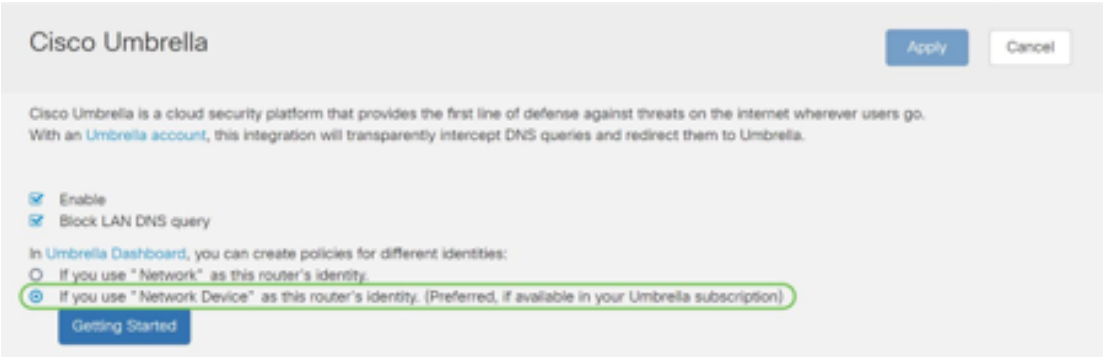


Etapa 3 (Opcional)

Por padrão, a caixa *Bloquear consultas DNS de LAN* está selecionada. Esse recurso de rede cria automaticamente listas de controle de acesso no roteador, o que impedirá que o tráfego DNS saia para a Internet. Este recurso força todas as solicitações de tradução de domínio a serem direcionadas através do RV345P e é uma boa ideia para a maioria dos usuários.

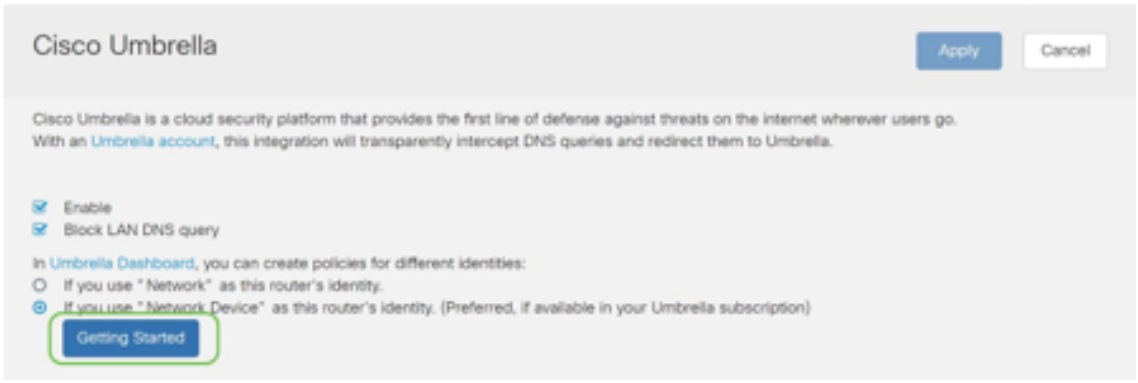
Passo 4

O próximo passo é executado de duas maneiras diferentes. Ambos dependem da configuração da sua rede. Se você usa um serviço como DynDNS ou NoIP, deixa o esquema de nomes padrão de "Rede". Você precisará fazer login nessas contas para garantir as interfaces Umbrella com esses serviços, pois ele oferece proteção. Para nossos propósitos, estamos confiando no "dispositivo de rede", então clicamos no botão de opção inferior.



Etapa 5

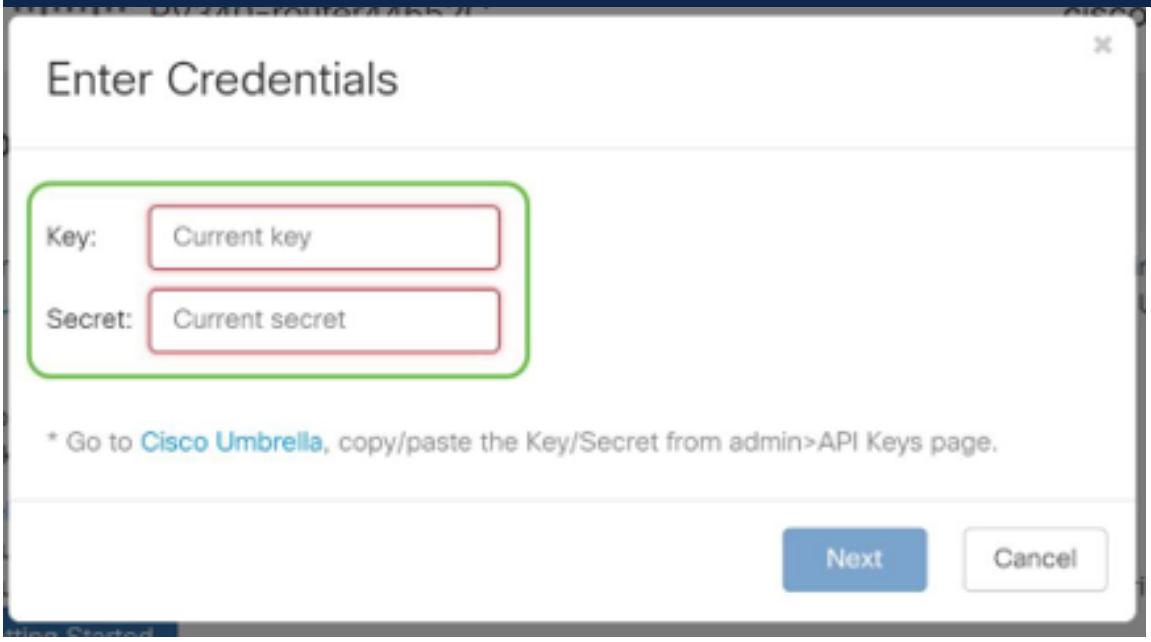
Clique em **Getting Started (Introdução)**.



Etapa 6

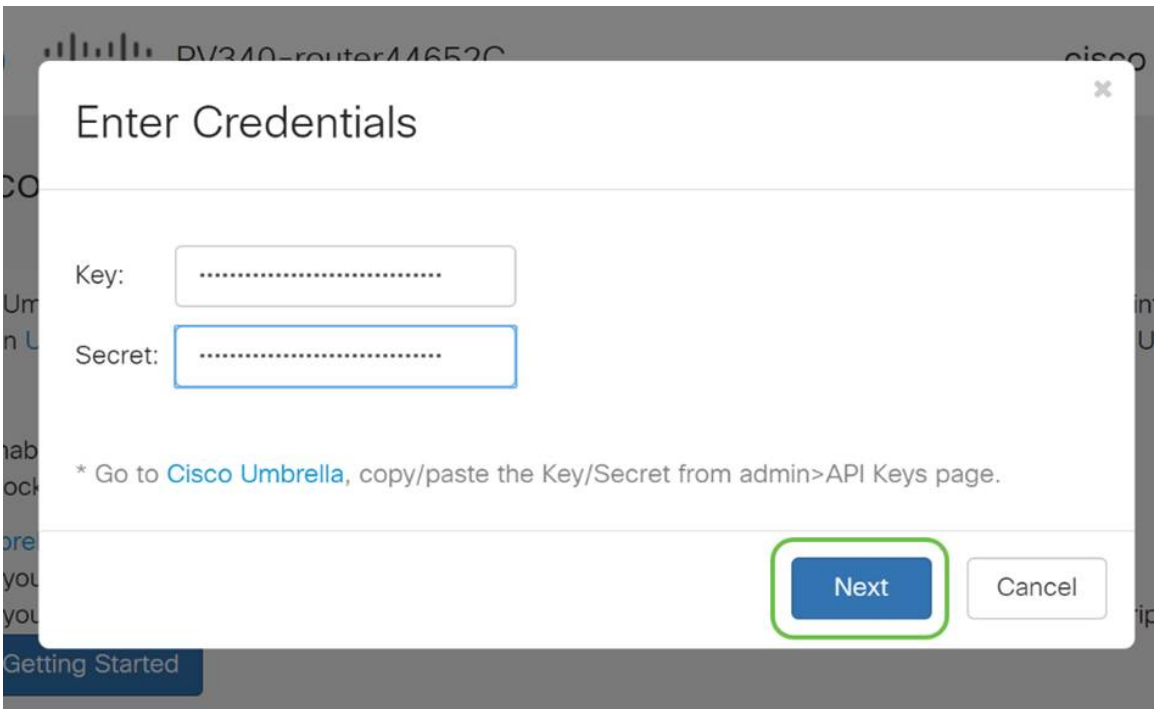
Insira a **chave da API** e a **chave secreta** nas caixas de texto.

Ligar duas vezes para você saber que é importante! Se você perder ou excluir acidentalmente a chave secreta, não há nenhuma função ou número de suporte para ligar para recuperar essa chave. Mantenha segredo e seguro. Se perdido, você precisará excluir a chave e reautorizar a nova chave API com cada dispositivo que deseja proteger com o Umbrella.



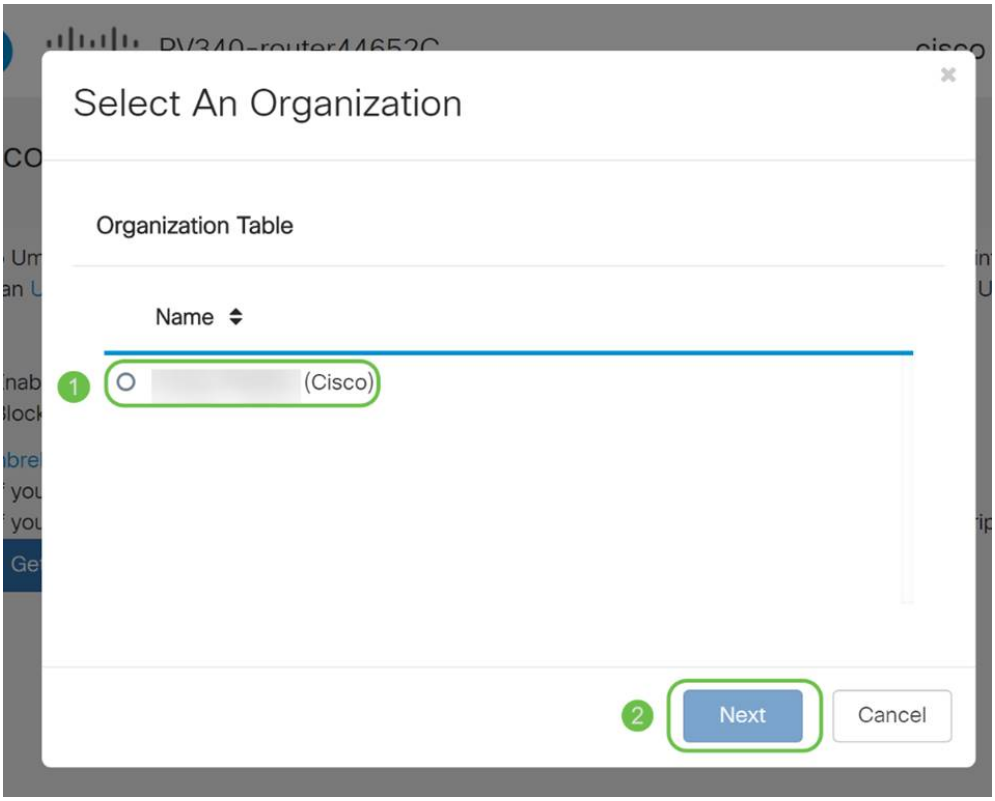
Etapa 7

Depois de inserir sua API e chave secreta, clique no botão **Avançar**.



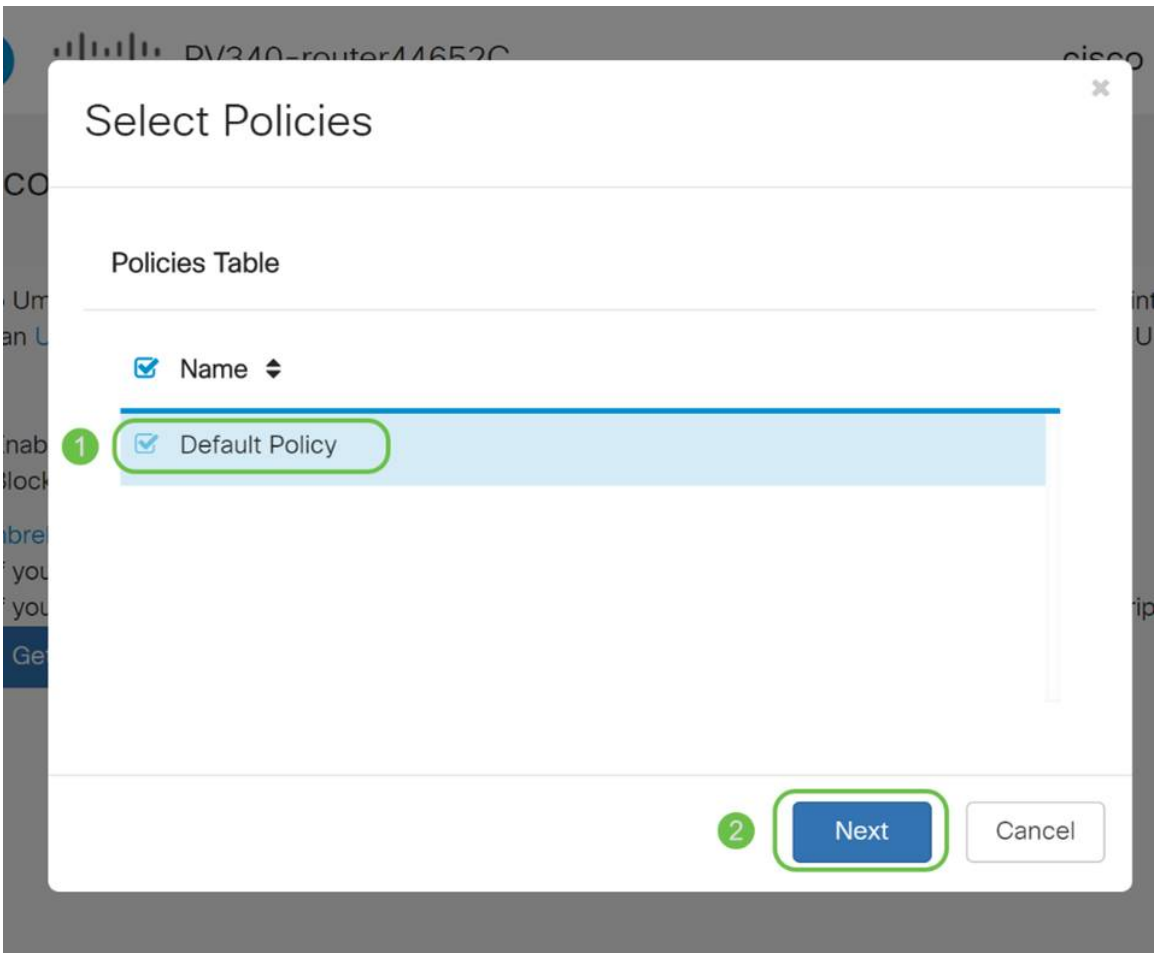
Passo 8

Na próxima tela, selecione a **organização** que deseja associar ao roteador. Clique em Next.



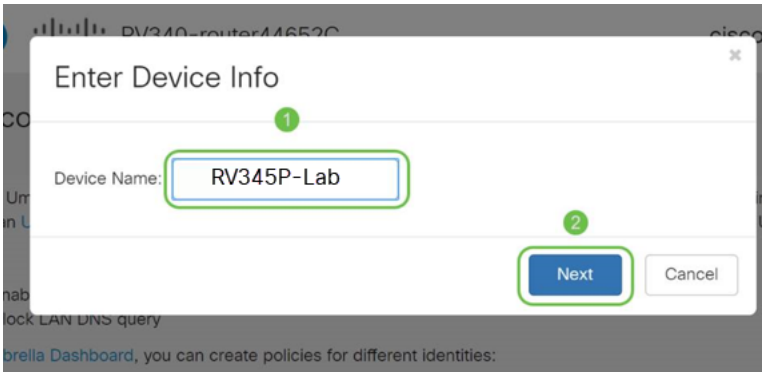
Passo 9

Selecione a política a ser aplicada ao tráfego roteado pelo RV345P. Para a maioria dos usuários, a política padrão fornecerá cobertura suficiente.



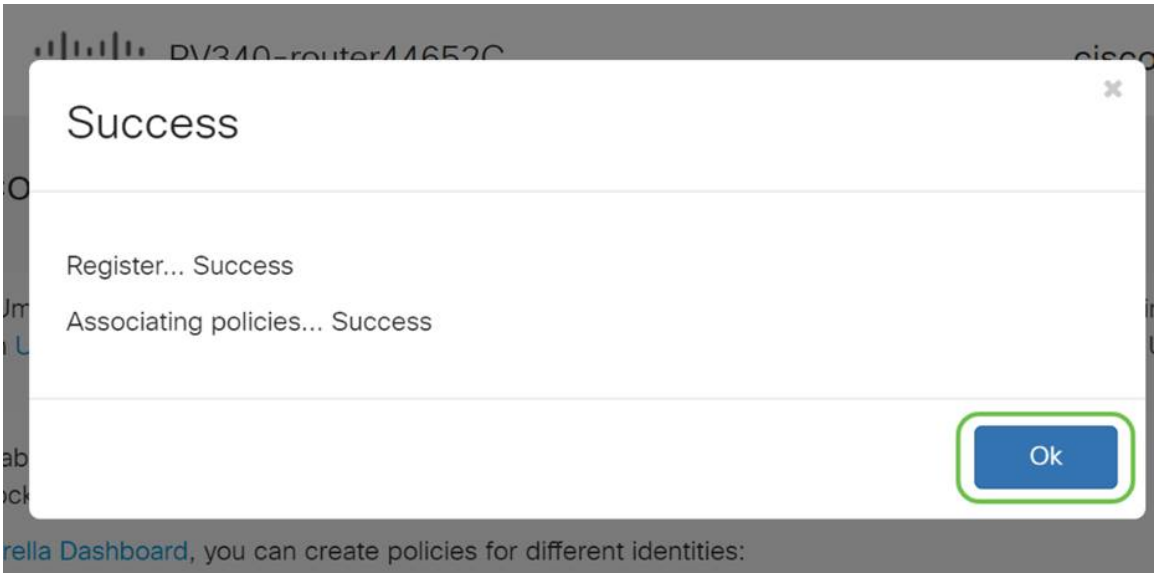
Passo 10

Atribua um nome ao dispositivo para que ele possa ser designado nos relatórios do Umbrella. Em nossa configuração, nós o nomeamos *RV345P-Lab*.



Passo 11

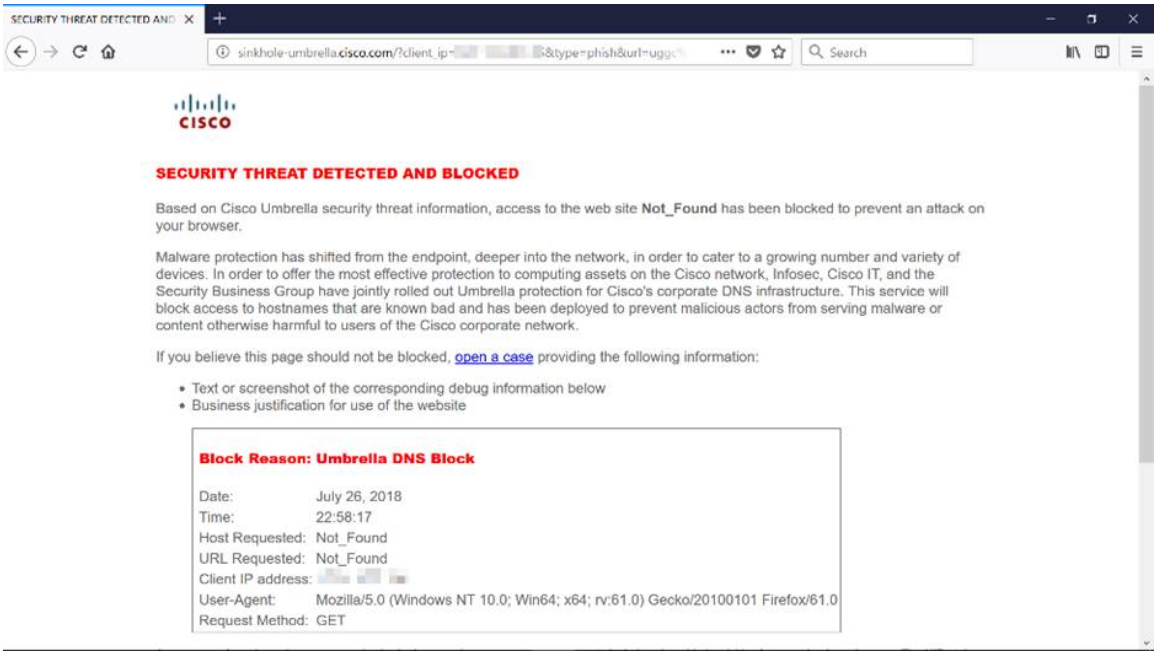
A próxima tela validará as configurações escolhidas e fornecerá uma atualização quando associada com êxito. Click OK.



Confirmação

Parabéns, agora você está protegido pelo Cisco Umbrella. Ou você é? Certifique-se de que, verificando duas vezes um exemplo ao vivo, a Cisco criou um site dedicado a determinar isso tão rapidamente quanto a página é carregada. Clique aqui ou digite https://InternetBadGuys.com na barra do navegador.

Se o Umbrella estiver configurado corretamente, você será saudado por uma tela semelhante a esta.



Outras opções de segurança

Você está preocupado que alguém tente acessar a rede sem autorização desconectando um cabo Ethernet de um dispositivo de rede e conectando-se a ele? Nesse caso, é importante registrar uma lista de hosts permitidos para se conectar diretamente ao roteador com seus respectivos endereços IP e MAC. As instruções podem ser encontradas no artigo Configure IP Source Guard on the RV34x Series Router.

Opções de VPN

Uma conexão VPN (Virtual Private Network) permite que os usuários acessem, enviem e recebam dados de e para uma rede privada por meio de uma rede pública ou compartilhada, como a Internet, mas ainda garantindo uma conexão segura com uma infraestrutura de rede subjacente para proteger a rede privada e seus recursos.

Um túnel VPN estabelece uma rede privada que pode enviar dados com segurança usando criptografia e autenticação. Os escritórios corporativos usam principalmente a conexão VPN, pois ela é útil e necessária para permitir que seus funcionários tenham acesso à sua rede privada mesmo que estejam fora do escritório.

A VPN permite que um host remoto atue como se estivesse localizado na mesma rede local. O roteador suporta até 50 túneis. Uma conexão VPN pode ser configurada entre o roteador e um endpoint depois que o roteador tiver sido configurado para conexão com a Internet. O cliente VPN depende inteiramente das configurações do roteador VPN para poder estabelecer uma conexão.

Se não tiver certeza de qual VPN melhor atende às suas necessidades, consulte Visão geral do Cisco Business VPN e Melhores práticas.

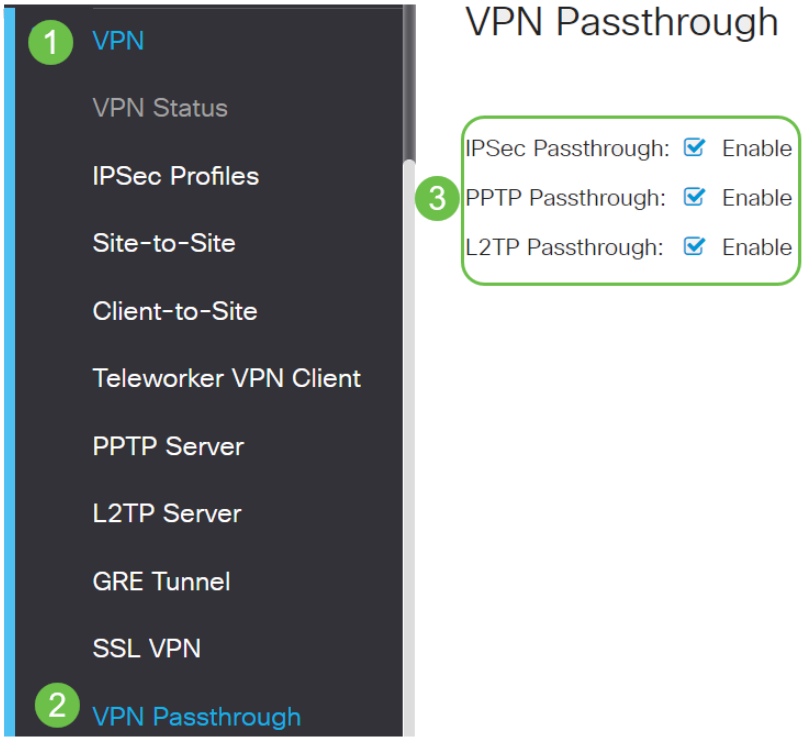
O AnyConnect VPN é o único produto compatível com Cisco VPN listado neste guia de configuração. Produtos de terceiros, que não sejam da Cisco, incluindo o TheGreenBow e o Shrew Soft não são suportados pela Cisco. São incluídos estritamente para fins de orientação. Se precisar de suporte sobre esses itens além do artigo, entre em contato com o terceiro para obter suporte.

Se não estiver planejando configurar uma VPN, você poderá clicar para ir para a próxima seção.

Passagem de VPN

Geralmente, cada roteador suporta Network Address Translation (NAT) para conservar endereços IP quando você deseja suportar vários clientes com a mesma conexão de Internet. No entanto, o Point-to-Point Tunneling Protocol (PPTP) e o IPsec (Internet Protocol Security) VPN não suportam NAT. É aqui que entra a passagem de VPN. Uma passagem de VPN é um recurso que permite que o tráfego de VPN gerado de clientes VPN conectados a esse roteador passe por esse roteador e se conecte a um ponto de extremidade de VPN. A passagem de VPN permite que o PPTP e o IPsec VPN apenas passem pela Internet, que é iniciada a partir de um cliente VPN, e então acessem o gateway VPN remoto. Esse recurso é comumente encontrado em roteadores domésticos que suportam NAT.

Por padrão, a passagem IPsec, PPTP e L2TP estão ativadas. Se quiser visualizar ou ajustar essas configurações, selecione **VPN > VPN Passthrough**. Visualize ou ajuste conforme necessário.



AnyConnect VPN

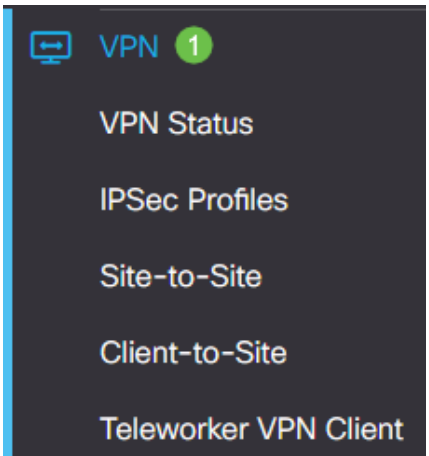
Há várias vantagens em usar o Cisco AnyConnect:

1. Conectividade segura e persistente
2. Segurança persistente e aplicação de políticas
3. Implantável a partir do Adaptive Security Appliance (ASA) ou de sistemas de implantação de software empresarial
4. Personalizável e traduzível
5. Facilmente configurado
6. Suporta IPsec (Internet Protocol Security) e SSL (Secure Sockets Layer)
7. Suporta o protocolo IKEv2.0 (Internet Key Exchange versão 2.0)

Configurar o AnyConnect SSL VPN no RV345P

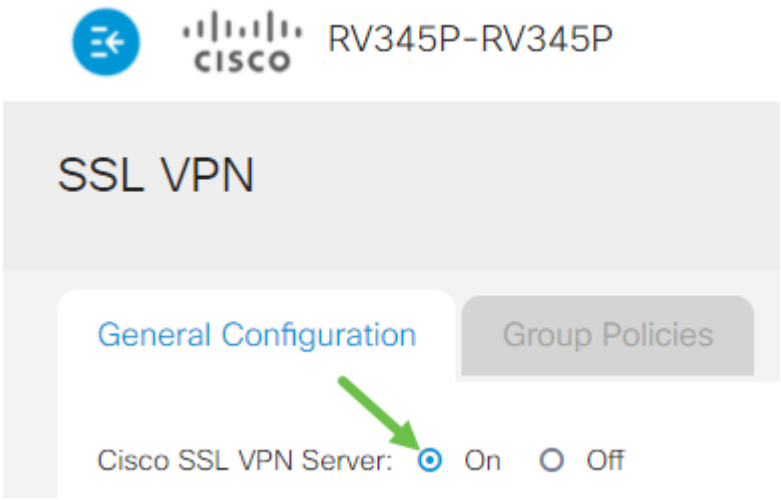
Passo 1

Acesse o utilitário baseado na Web do roteador e escolha **VPN > SSL VPN**.



Passo 2

Clique no botão de opção **On** (Ativado) para habilitar o Cisco SSL VPN Server.



Configurações obrigatórias do gateway

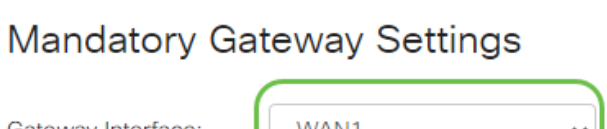
Passo 1

As seguintes configurações são obrigatórias:

1. Escolha a interface do gateway na lista suspensa. Esta será a porta que será usada para passar o tráfego através dos túneis VPN SSL. As opções incluem: WAN1, WAN2, USB1, USB2
2. Insira o número da porta que é usada para o gateway de VPN SSL no campo Porta do Gateway que varia de 1 a 65535.
3. Escolha o Arquivo de certificado na lista suspensa. Este certificado autentica os usuários que tentam acessar o recurso de rede através dos túneis VPN SSL. A lista suspensa contém um certificado padrão e os certificados importados.
4. Insira o endereço IP do pool de endereços do cliente no campo *Client Address Pool*. Esse pool será o intervalo de endereços IP que serão alocados para clientes VPN remotos.

   Certifique-se de que o intervalo de endereços IP não se sobreponha a nenhum dos endereços IP na rede local.

6. Escolha a máscara de rede do cliente na lista suspensa.
7. Digite o nome de domínio do cliente no campo *Domínio do cliente*. Esse será o nome de domínio que deve ser enviado para clientes VPN SSL.
8. Insira o texto que apareceria como um banner de login no campo *Banner de login*. Este será o banner que será exibido toda vez que um cliente fizer login.



Passo 2

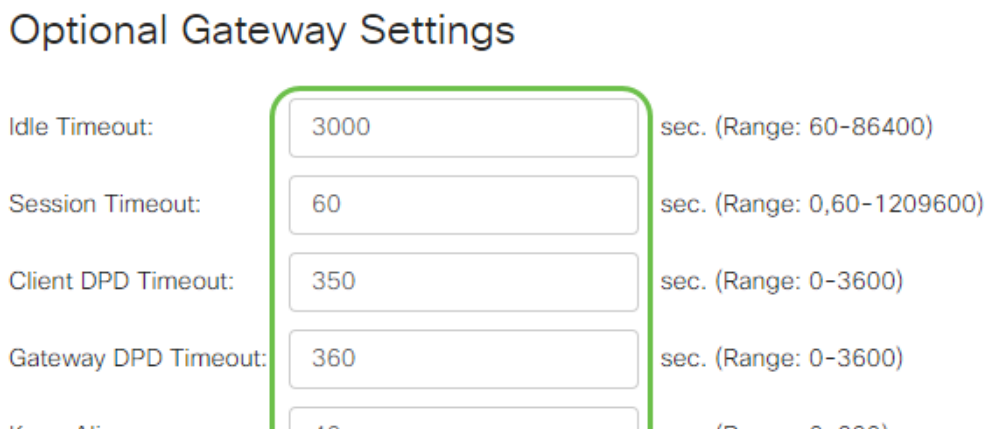
Clique em Apply.

Configurações opcionais do gateway

Passo 1

As seguintes configurações são opcionais:

1. Insira um valor em segundos para o intervalo de tempo limite de ociosidade de 60 a 86.400. Esta será a duração em que a sessão VPN SSL poderá permanecer ociosa.
2. Insira um valor em segundos no campo *Limite de tempo da sessão*. Esse é o tempo que leva para a sessão do Transmission Control Protocol (TCP) ou User Datagram Protocol (UDP) expirar após o tempo ocioso especificado. O intervalo é de 60 a 1209600.
3. Insira um valor em segundos no campo *ClientDPD Timeout* que varia de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN. Esse recurso deve ser ativado em ambas as extremidades do túnel VPN.
4. Insira um valor em segundos no campo *GatewayDPD Timeout* que varia de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN. Esse recurso deve ser ativado em ambas as extremidades do túnel VPN.
5. Insira um valor em segundos no campo *Keep Alive* que varia de 0 a 600. Esse recurso garante que o roteador esteja sempre conectado à Internet. Tentará restabelecer a conexão VPN se for interrompida.
6. Insira um valor em segundos para a duração do túnel a ser conectado no campo *Duração da concessão*. O intervalo é de 600 a 1209600.
7. Insira o tamanho do pacote em bytes que pode ser enviado pela rede. O intervalo é de 576 a 1406.
8. Insira o tempo do intervalo de retransmissão no campo *Intervalo de rechave*. O recurso Rekey permite que as chaves SSL renegociem após a sessão ter sido estabelecida. O intervalo é de 0 a 43200.



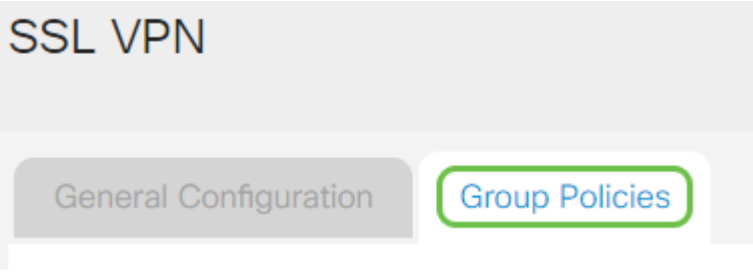
Passo 2

Clique em Apply.

Configurar políticas de grupo

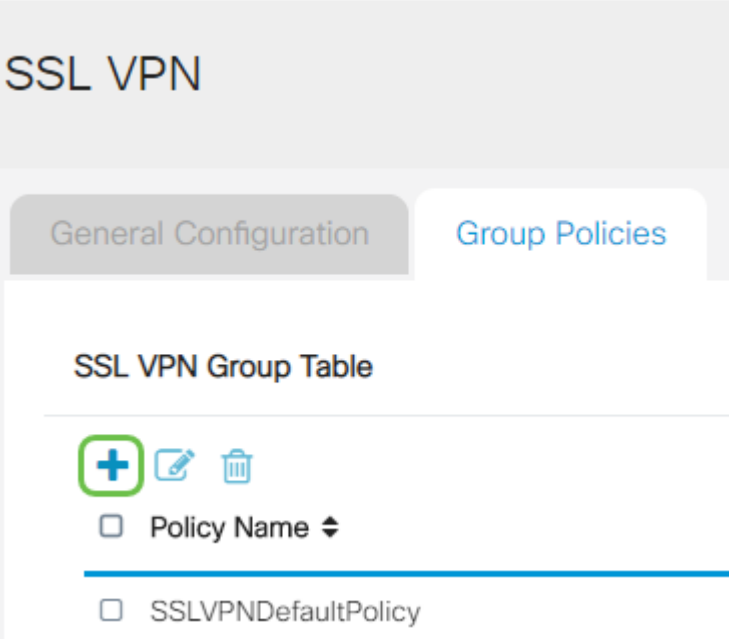
Passo 1

Clique na guia **Group Policies**.



Passo 2

Clique no **ícone Add** na Tabela de grupos de VPN SSL para adicionar uma política de grupo.

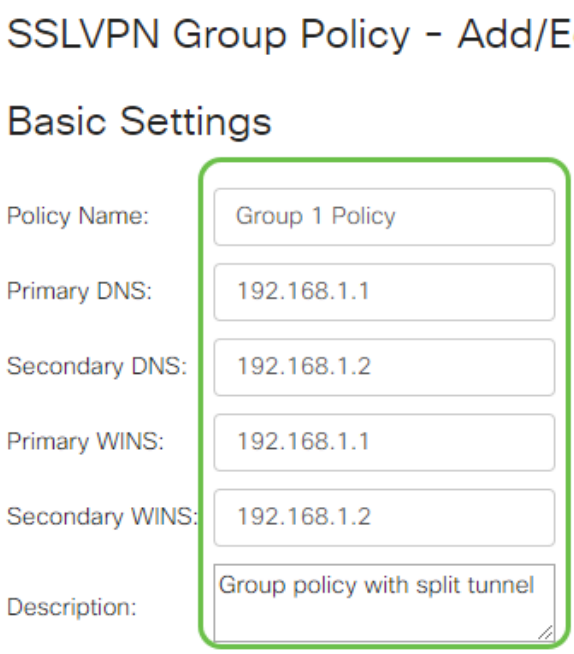


A tabela Grupo de VPN SSL exibirá a lista de políticas de grupo no dispositivo. Você também pode editar a primeira política de grupo na lista, que é chamada SSLVPNDefaultPolicy. Essa é a política padrão fornecida pelo dispositivo.

Etapa 3

1. Digite o nome da política preferida no campo *Nome da política*.

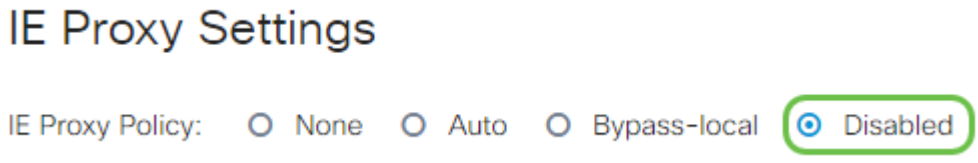
2. Insira o endereço IP do DNS primário no campo fornecido. Por padrão, esse endereço IP já é fornecido.
3. *(Opcional) Insira o endereço IP do DNS secundário no campo fornecido. Isso servirá como backup caso o DNS primário falhe.*
4. (Opcional) Insira o endereço IP do WINS principal no campo fornecido.
5. (Opcional) Insira o endereço IP do WINS secundário no campo fornecido.
6. (Opcional) Insira uma descrição da política no campo *Descrição*.



Etapa 4 (Opcional)

Clique em um botão de opção para escolher a Política de Proxy do IE para habilitar as configurações de proxy do Microsoft Internet Explorer (MSIE) para estabelecer um túnel VPN. As opções são:

- Nenhum - Permite que o navegador não use configurações de proxy.
- Auto - Permite que o navegador detecte automaticamente as configurações de proxy.
- Bypass-local - Permite que o navegador ignore as configurações de proxy configuradas no usuário remoto.
- Desativado - Desativa as configurações de proxy MSIE.



Etapa 5 (opcional)

Na área Configurações de tunelamento dividido, marque a caixa de seleção **Habilitar tunelamento dividido** para permitir que o tráfego destinado à Internet seja enviado sem criptografia diretamente para a Internet. O tunelamento completo envia todo o tráfego para o dispositivo final, onde é roteado para os recursos de destino, eliminando a rede

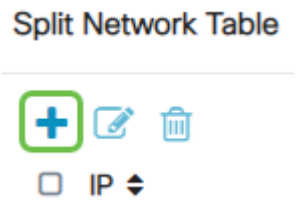
corporativa do caminho para acesso à Web.

Etapa 6 (Opcional)

Clique em um botão de opção para escolher incluir ou excluir tráfego ao aplicar o tunelamento dividido.

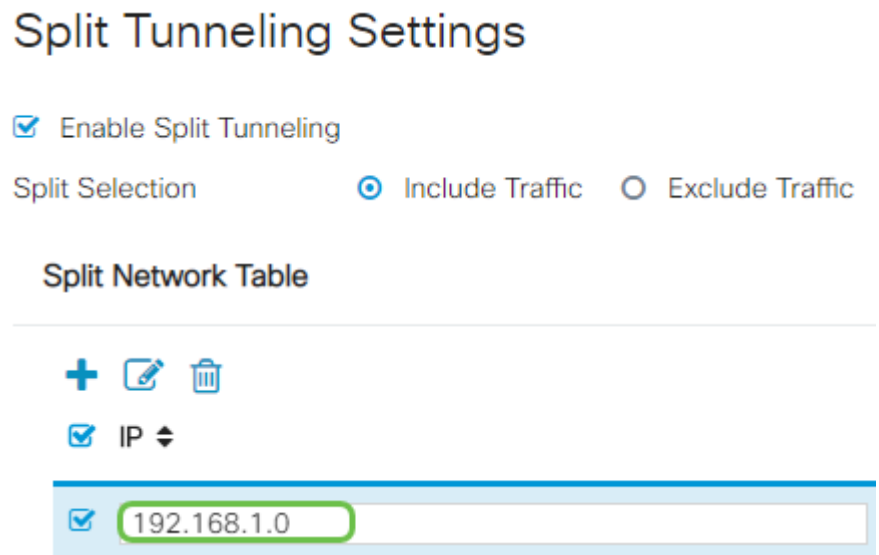
Etapa 7

Na Tabela de divisão de rede, clique no **ícone Adicionar** para adicionar uma exceção de divisão de rede.



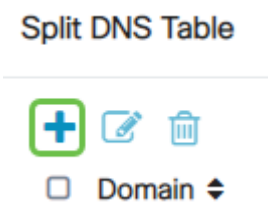
Passo 8

Insira o endereço IP da rede no campo fornecido.



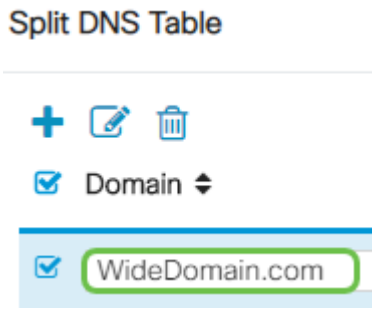
Passo 9

Na Tabela de DNS dividido, clique no **ícone Adicionar** para adicionar uma exceção de DNS dividido.



Passo 10

Insira o nome do domínio no campo fornecido e clique em **Apply**.



Por padrão, o roteador vem com 2 licenças de servidor do AnyConnect. Isso significa que, uma vez que você tenha licenças de cliente do AnyConnect, poderá estabelecer 2 túneis VPN simultaneamente com qualquer outro roteador da série RV340.

Resumindo, o roteador RV345P não precisa de uma licença, mas todos os clientes precisarão de uma. As licenças do cliente AnyConnect permitem que clientes móveis e desktop acessem a rede VPN remotamente.

Esta próxima seção detalha como obter licenças para seus clientes.

AnyConnect Mobility Client

Um cliente VPN é um software instalado e executado em um computador que deseja se conectar à rede remota. Esse software cliente deve ser configurado com a mesma configuração do servidor VPN, como o endereço IP e as informações de autenticação. Essas informações de autenticação incluem o nome de usuário e a chave pré-compartilhada que serão usados para criptografar os dados. Dependendo da localização física das redes a serem conectadas, um cliente VPN também pode ser um dispositivo de hardware. Isso geralmente acontece se a conexão VPN for usada para conectar duas redes que estão em locais separados.

O Cisco AnyConnect Secure Mobility Client é um aplicativo de software para conexão a uma VPN que funciona em vários sistemas operacionais e configurações de hardware. Esse aplicativo de software permite que os recursos remotos de outra rede se tornem acessíveis como se o usuário estivesse diretamente conectado à sua rede, mas de forma segura.

Depois que o roteador estiver registrado e configurado com o AnyConnect, o cliente poderá instalar licenças no roteador a partir do pool de licenças disponíveis que você adquire, detalhado na próxima seção.

Licença de compra

Você deve adquirir uma licença do seu distribuidor da Cisco ou do seu parceiro da Cisco. Ao solicitar uma licença, você deve fornecer a ID da sua Conta inteligente da Cisco ou a ID do domínio na forma de *name@domain.com*.

Se você não tiver um distribuidor ou parceiro da Cisco, poderá localizar um aqui.

No momento da elaboração, as seguintes SKUs de produto podem ser usadas para comprar licenças adicionais em pacotes de 25. Observe que há outras opções para as licenças de clientes do AnyConnect, conforme descrito no Guia de pedidos do Cisco AnyConnect, no entanto, a ID do produto listada seria o requisito mínimo para funcionalidade completa.

Observe que a SKU do produto de licença do cliente AnyConnect listada primeiro, fornece licenças por um período de 1 ano e exige uma compra mínima de 25 licenças. Outras SKUs de produto aplicáveis aos roteadores da série RV340 também estão disponíveis com níveis de assinatura variados, como a seguir:

- **LS-AC-PLS-1Y-S1** — licença de cliente Cisco AnyConnect Plus de 1 ano
- **LS-AC-PLS-3Y-S1** — licença de cliente Cisco AnyConnect Plus de 3 anos
- **LS-AC-PLS-5Y-S1** — licença de cliente Cisco AnyConnect Plus de 5 anos
- **LS-AC-PLS-P-25-S** — pacote de 25 licenças de cliente vitalícias do Cisco AnyConnect Plus
- **LS-AC-PLS-P-50-S** — pacote de 50 licenças de cliente vitalícias do Cisco AnyConnect Plus

Informações do cliente

Quando seu cliente configurar um dos seguintes itens, você deve enviar a eles estes links:

- Windows: AnyConnect em um computador Windows
- Mac: Instale o AnyConnect no Mac.
- Desktop do Ubuntu: Instalação e uso do AnyConnect no desktop Ubuntu
- Se tiver problemas, você pode ir para Coletar informações para solução de problemas básicos em erros do Cisco AnyConnect Secure Mobility Client.

Verificar a conectividade do AnyConnect VPN

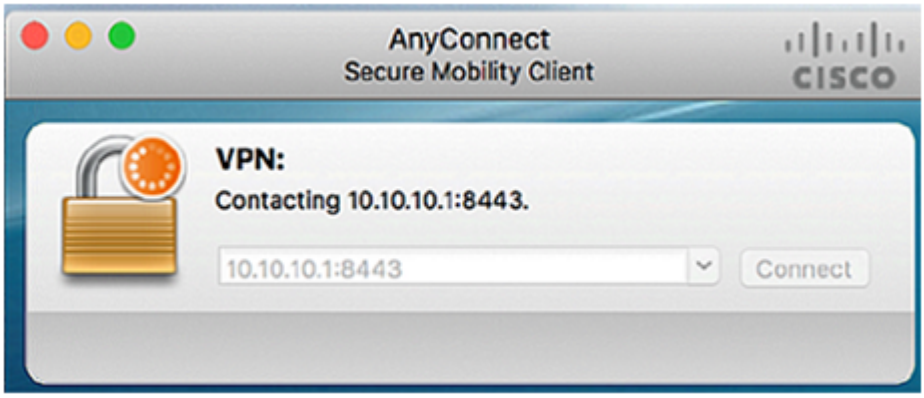
Passo 1

Clique no **ícone do AnyConnect Secure Mobility Client**.

Passo 2

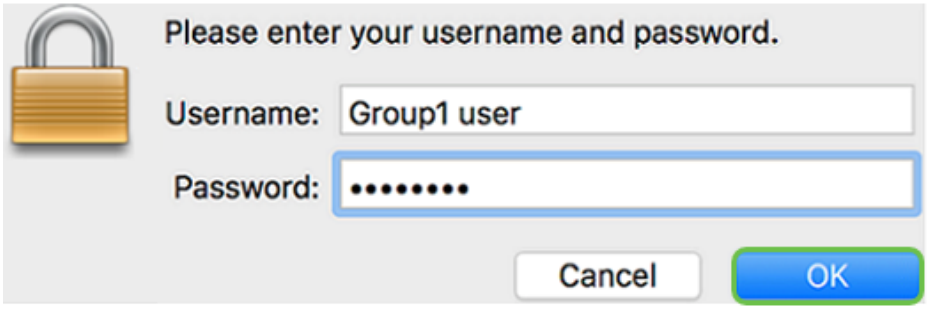
Na janela AnyConnect Secure Mobility Client, insira o endereço IP do gateway e o número da porta do gateway separados por dois-pontos (:) e clique em **Connect**.

O software agora mostrará que está entrando em contato com a rede remota.



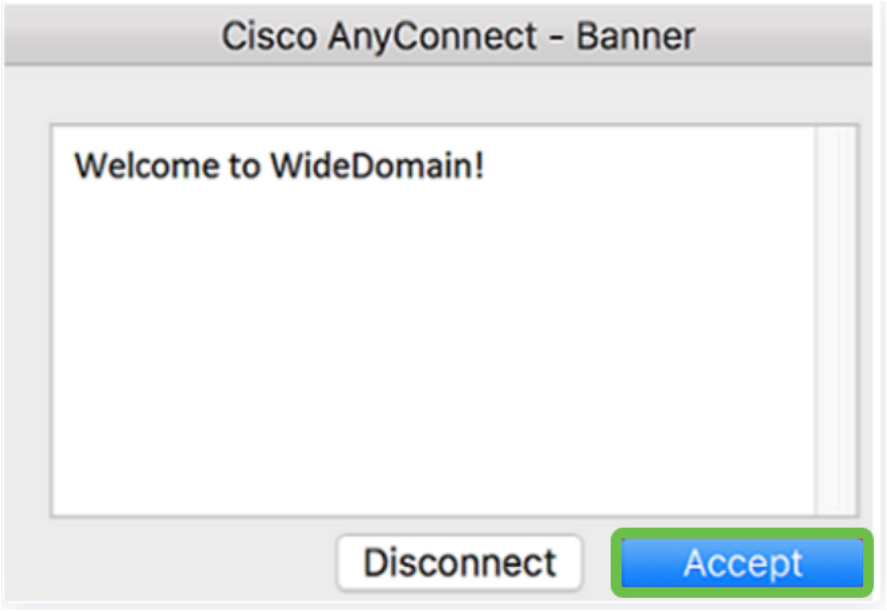
Etapa 3

Digite o nome de usuário e a senha do servidor nos respectivos campos e clique em **OK**.

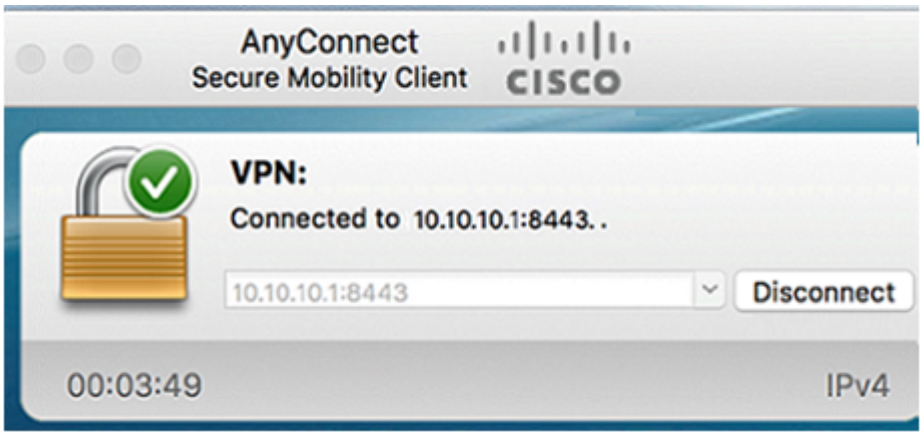


Passo 4

Assim que a conexão for estabelecida, o banner de login será exibido. Clique em **Aceitar**.



A janela do AnyConnect agora deve indicar a conexão VPN bem-sucedida com a rede.



Se agora estiver usando o AnyConnect VPN, você poderá ignorar outras opções de VPN e passar para a próxima seção.

Shrew Soft VPN

Uma VPN IPsec permite que você obtenha recursos remotos com segurança estabelecendo um túnel criptografado através da Internet. Os roteadores da série RV34X funcionam como servidores VPN IPsec e suportam o Shrew Soft VPN Client. Esta seção mostrará como configurar seu roteador e o Shrew Soft Client para proteger uma conexão a uma VPN.

A Cisco não oferece suporte à Shrew Soft. Este exemplo é fornecido somente para fins de demonstração. Se você tiver problemas com o Shrew Soft, entre em contato com eles para obter suporte.

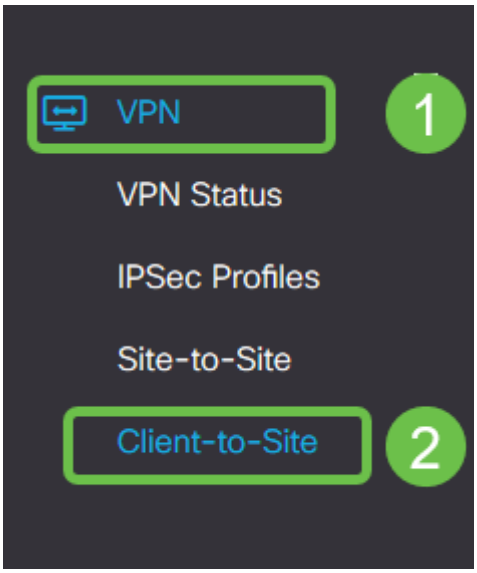
Você pode baixar a versão mais recente do software cliente Shrew Soft VPN aqui: https://www.shrew.net/download/vpn

Configurar Shrew Soft no RV345P Series Router

Começaremos configurando a **VPN Cliente a Local** no RV345P.

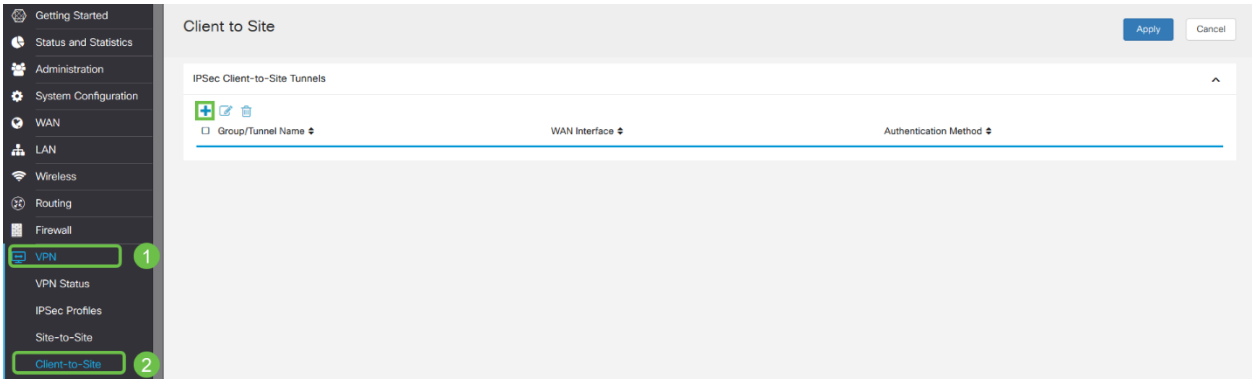
Passo 1

Navegue até **VPN > Cliente a site.**



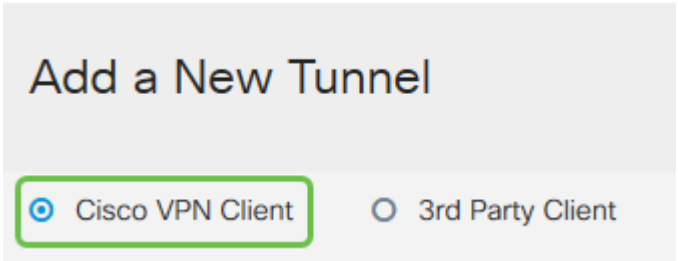
Passo 2

Adicione um perfil de VPN **Cliente a Site**.



Etapa 3

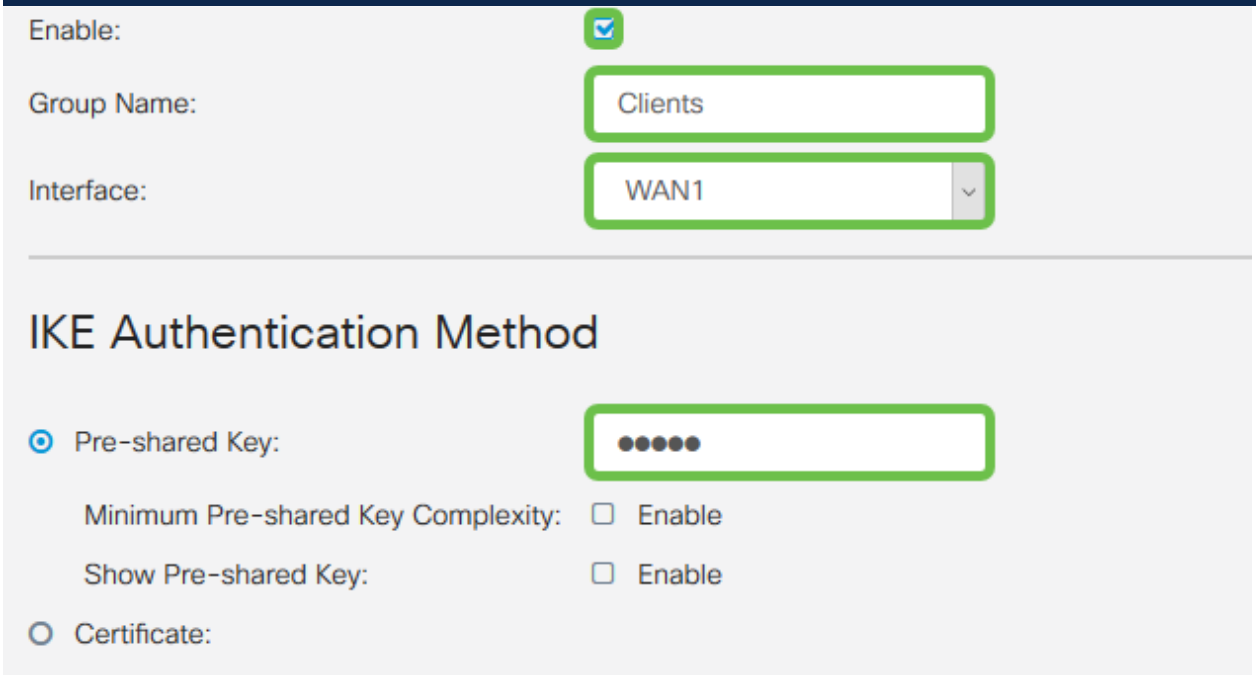
Selecione a opção **Cisco VPN Client**.



Passo 4

Marque a caixa **Enable** para ativar o VPN Client Profile. Também configuraremos o *nome do grupo*, selecionaremos a **interface WAN** e inseriremos uma **chave pré-compartilhada**.

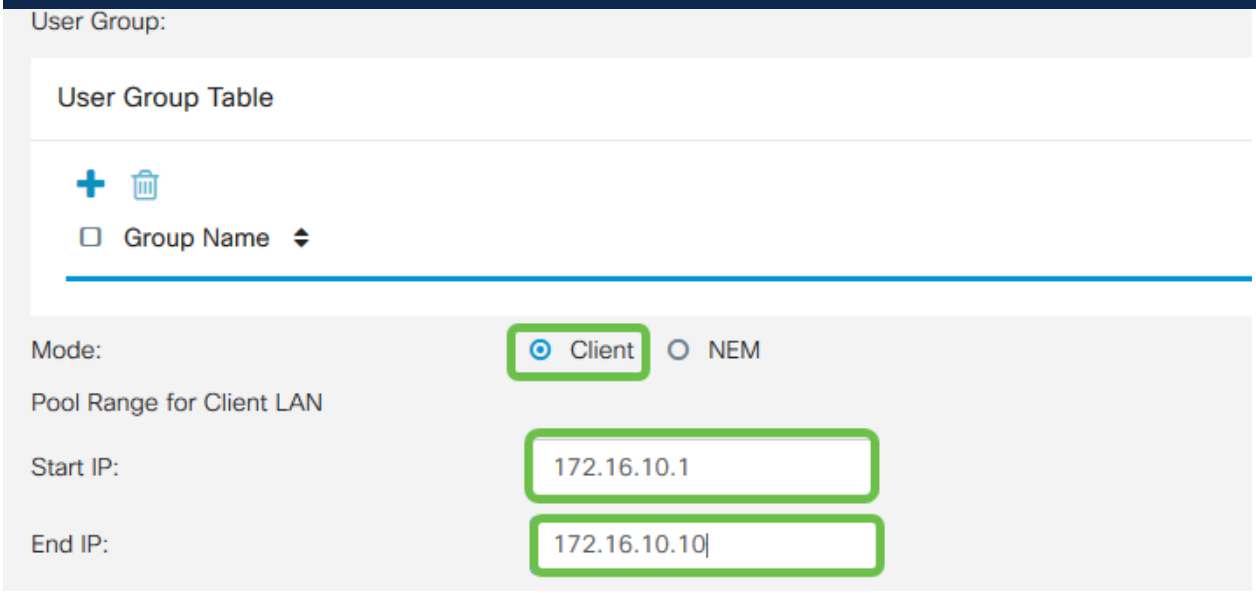
Anote o *nome do grupo* e a *chave pré-compartilhada*, pois eles serão usados mais tarde ao configurar o cliente.



Etapa 5

Deixe a **Tabela de grupos de usuários** em branco por enquanto. Isso é para o *Grupo de Usuários* no roteador, mas ainda não o configuramos. Verifique se **Mode** está definido como **Client**. Insira o **Intervalo de pool para LAN de cliente**. Usaremos 172.16.10.1 até 172.16.10.10.

O intervalo de pool deve usar uma sub-rede exclusiva que não seja usada em outro lugar da rede.

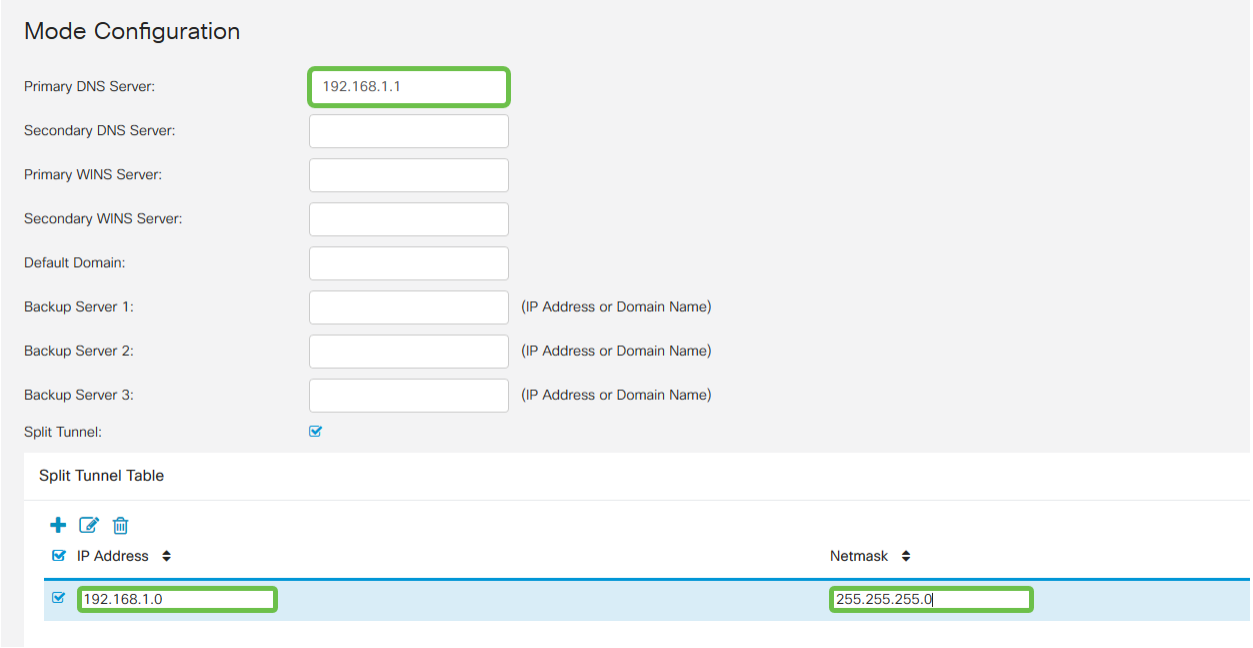


Etapa 6

Aqui é onde definimos as configurações **de configuração do modo**. Aqui estão as

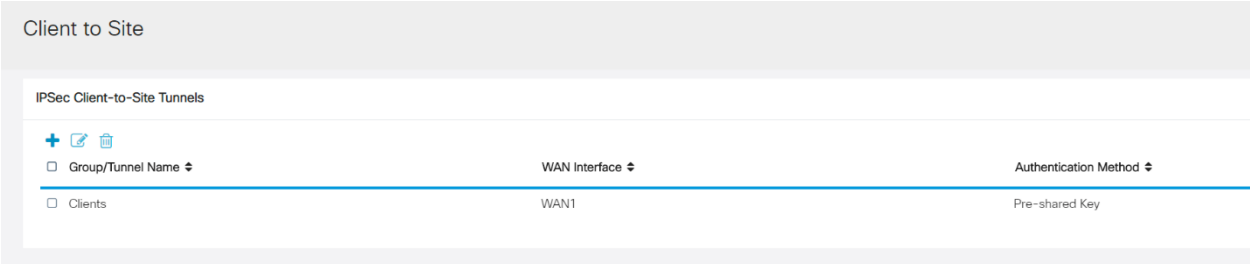
configurações que usaremos:

- **Servidor DNS primário**: Se você tiver um Servidor DNS interno ou quiser usar um Servidor DNS externo, você poderá inseri-lo aqui. Caso contrário, o padrão é o endereço IP da LAN RV345P. Usaremos o padrão em nosso exemplo.
- **Túnel dividido:** marque para ativar o tunelamento dividido. Isso é usado para especificar qual tráfego passará pelo túnel VPN. Usaremos o Split Tunnel em nosso exemplo.
- **Tabela de Túnel Dividido:** Insira as redes às quais o cliente VPN deve ter acesso através da VPN. Este exemplo usa a rede LAN RV345P.



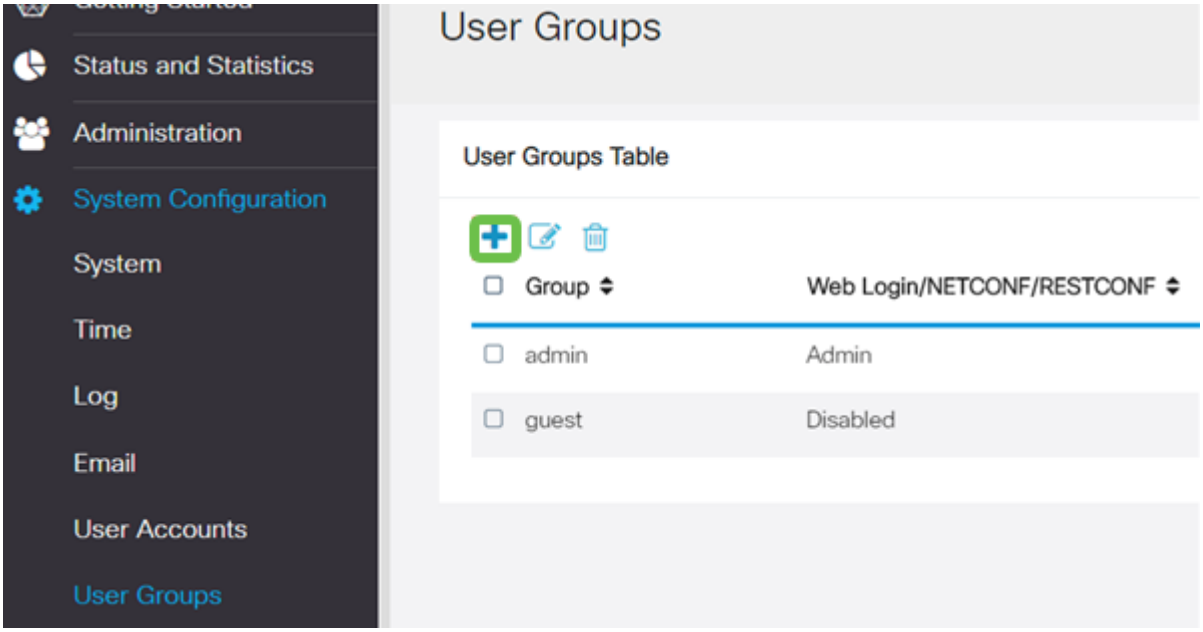
Etapa 7

Depois de clicar em **Salvar**, podemos ver o Perfil na lista **Grupos Cliente a Site IPsec**.



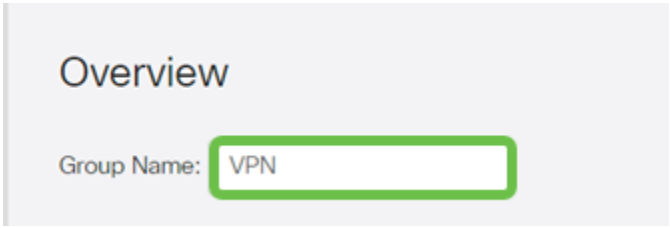
Passo 8

Configure um **grupo de usuários** para usar a autenticação de usuários de clientes VPN. Em **System Configuration > User Groups**, clique no **ícone de mais** para adicionar um User Group.



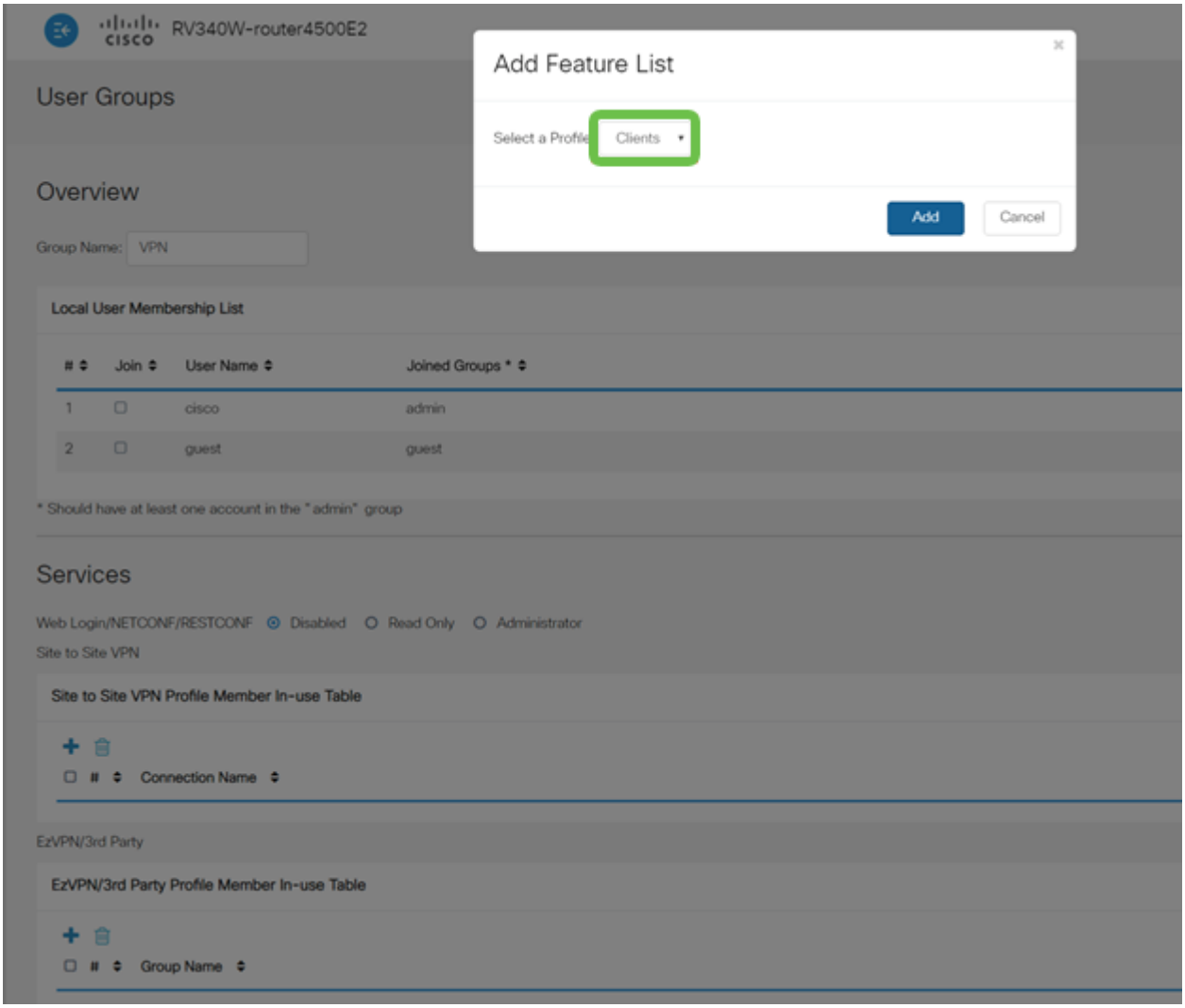
Passo 9

Digite um **nome de grupo**.



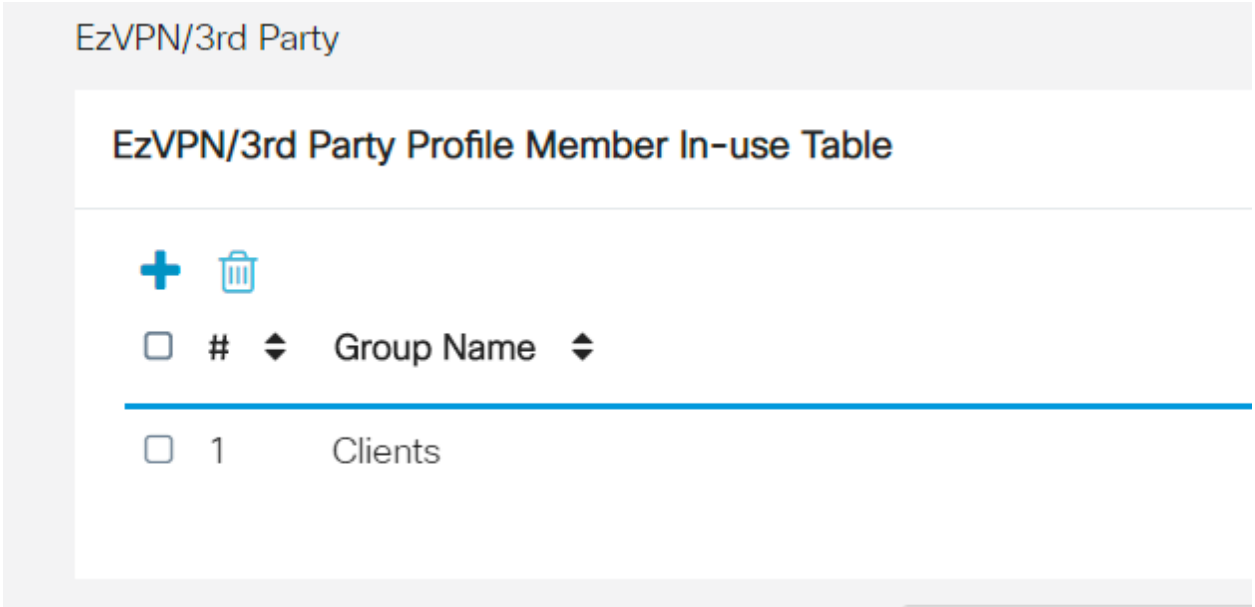
Passo 10

Em **Serviços > EzVPN/Terceiros**, clique em **Adicionar** para vincular este Grupo de Usuários ao Perfil **Cliente a Site** configurado anteriormente.



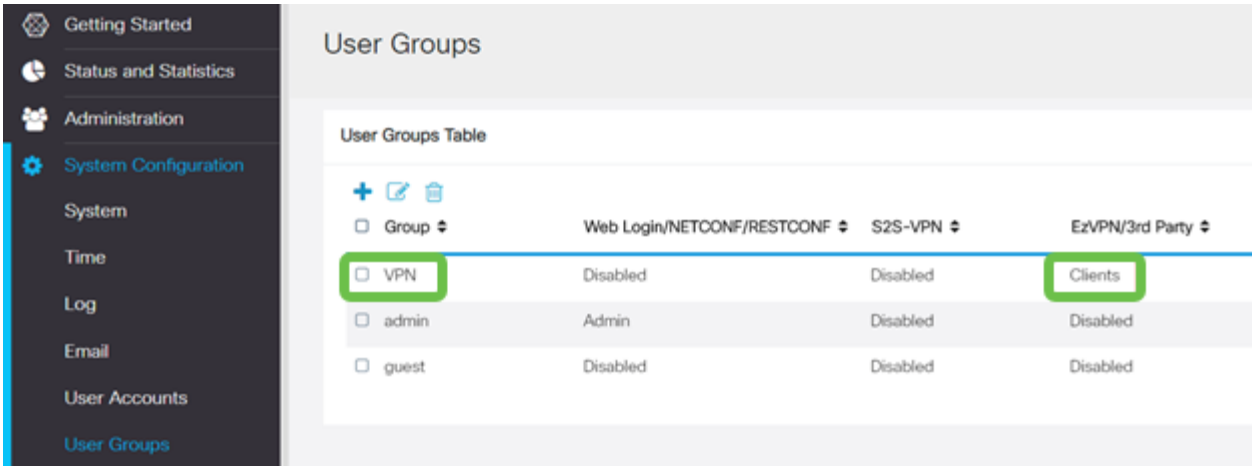
Passo 11

Agora você deve ver o nome do grupo **cliente a site** na lista para **EzVPN/terceiros.**



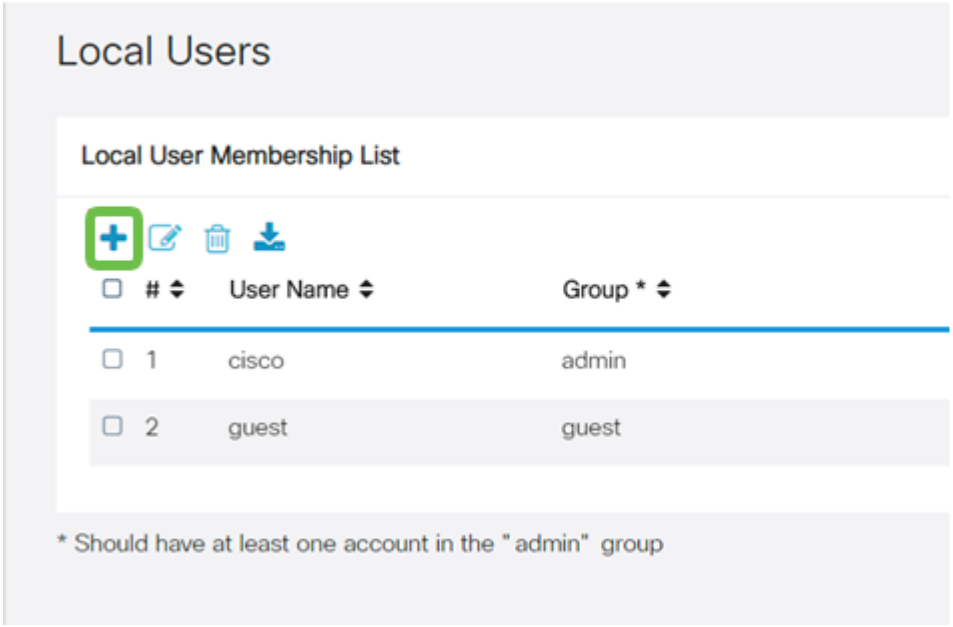
Etapa 12

Depois de **Aplicar** a configuração do Grupo de Usuários, você a verá na lista **Grupos de Usuários** e ela mostrará que o novo Grupo de Usuários será usado com o Perfil Cliente-Site criado anteriormente.



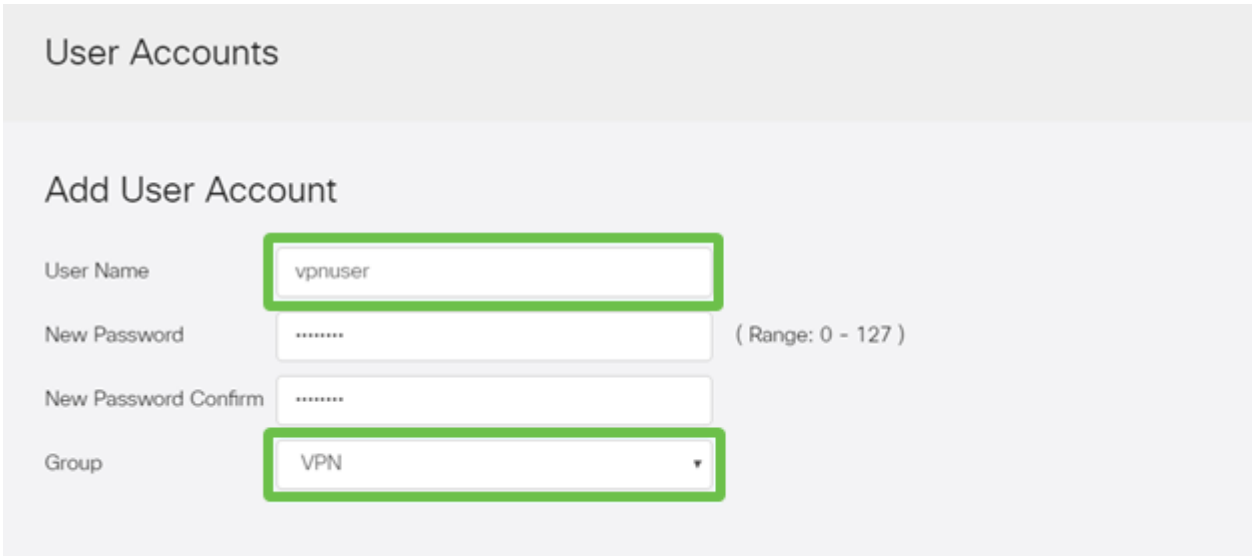
Passo 13

Configure um novo usuário em **System Configuration > User Accounts**. Clique no **ícone de mais** para criar um novo usuário.



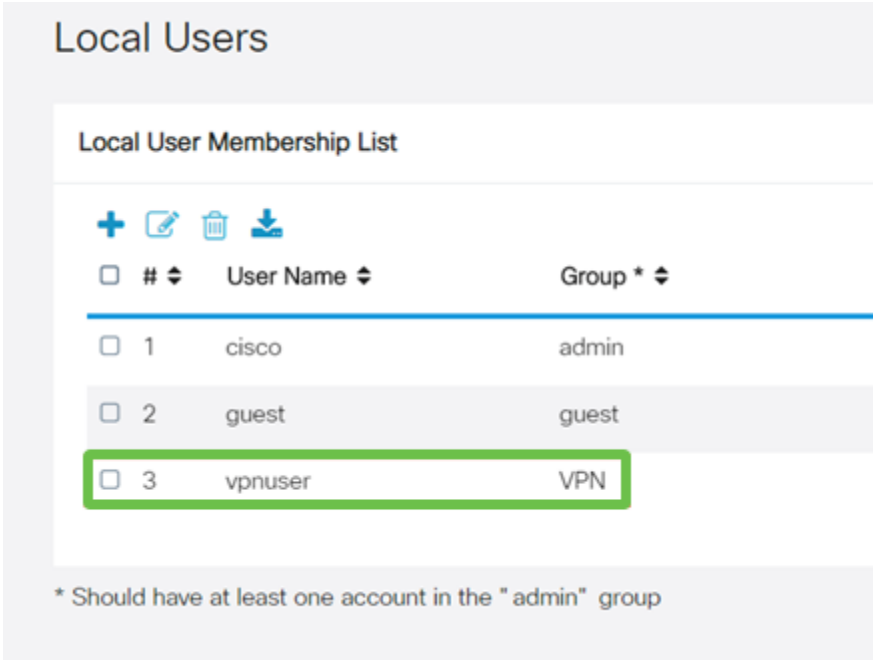
Passo 14

Insira o novo **Nome de usuário** junto com a **Nova senha**. Verifique se o **Grupo** está definido como o novo **Grupo de Usuários** que você acabou de configurar. Clique em **Apply** quando terminar.



Etapa 15

O novo **usuário** aparecerá na lista de **Usuários locais**.



Isso conclui a configuração no RV345P Series Router. Em seguida, você configurará o cliente Shrew Soft VPN.

Configurar o cliente Shrew Soft VPN

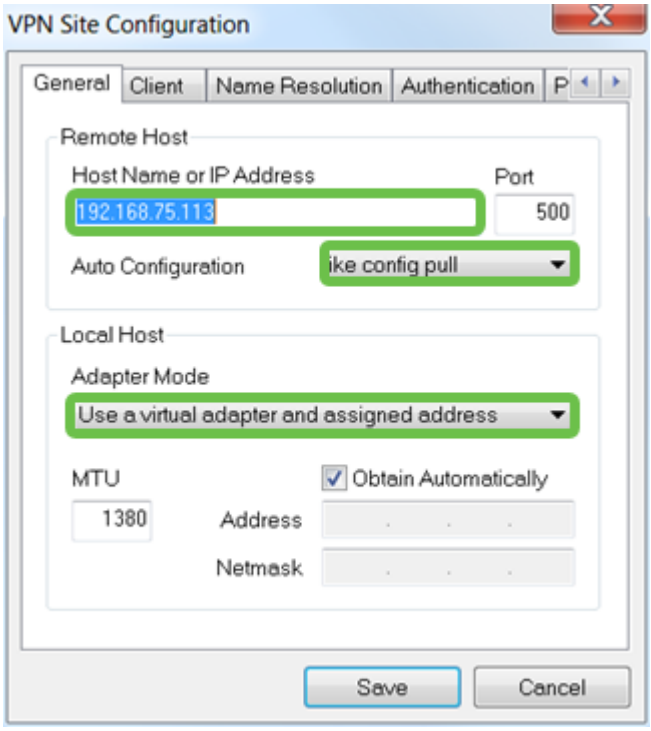
Execute as seguintes etapas.

Passo 1

Abra o *gerenciador de acesso VPN* de software Shrew e clique em **Adicionar** para adicionar um perfil. Na janela *VPN Site Configuration* exibida, configure a guia **General** :

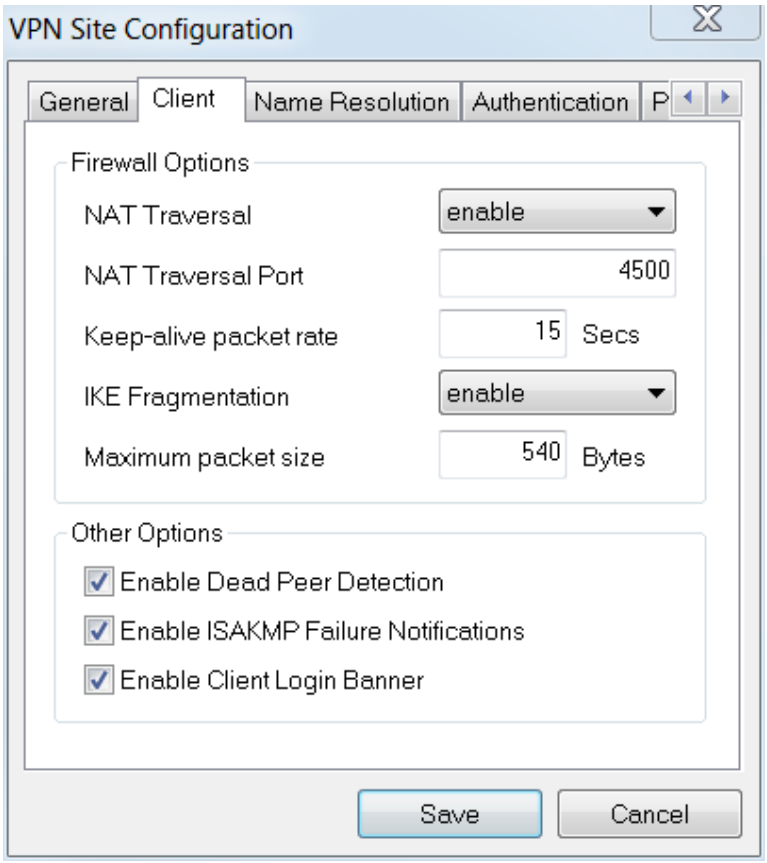
- **Nome do host ou endereço IP**: Usar o endereço IP da WAN (ou nome de host do RV345P)

- **Configuração automática**: Selecione **Ike config pull**
- **Modo do adaptador**: Selecione **Usar um adaptador virtual e endereço atribuído**



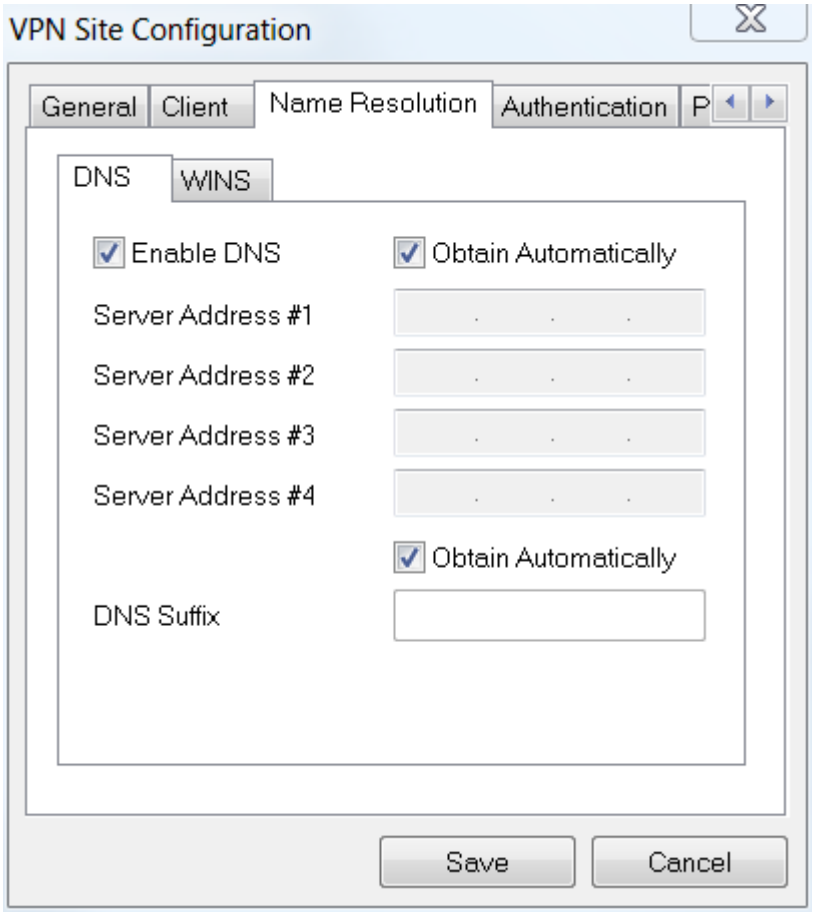
Passo 2

Configure a guia **Cliente**. Neste exemplo, mantivemos as configurações padrão.



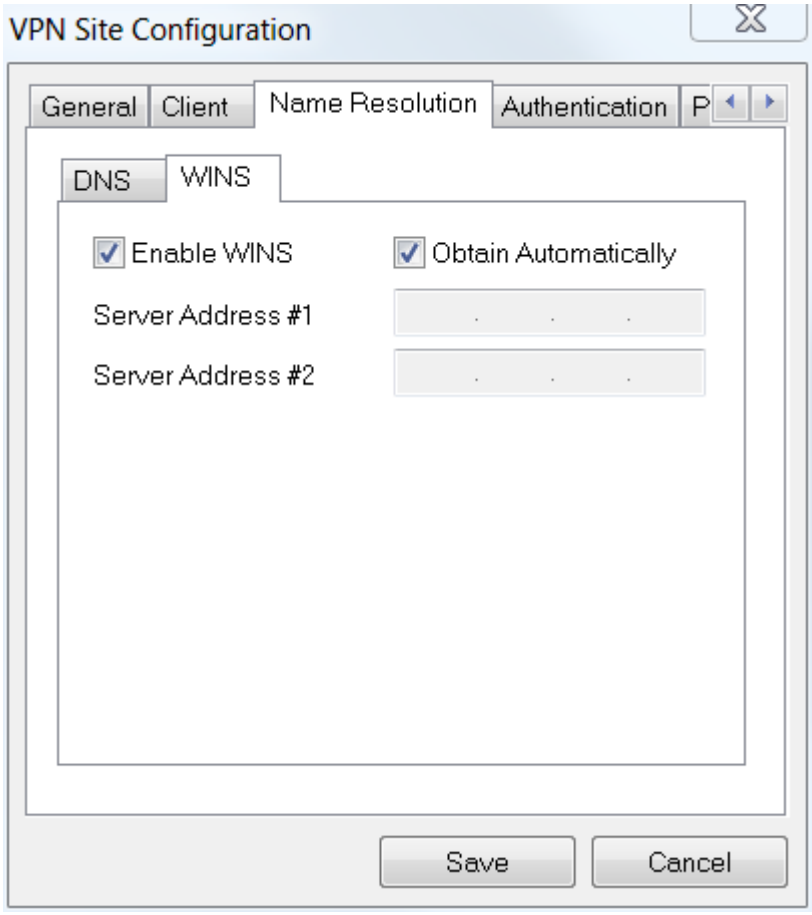
Etapa 3

Em **Resolução de nome > DNS**, marque a caixa **Habilitar DNS** e deixe as caixas **Obter automaticamente**.



Passo 4

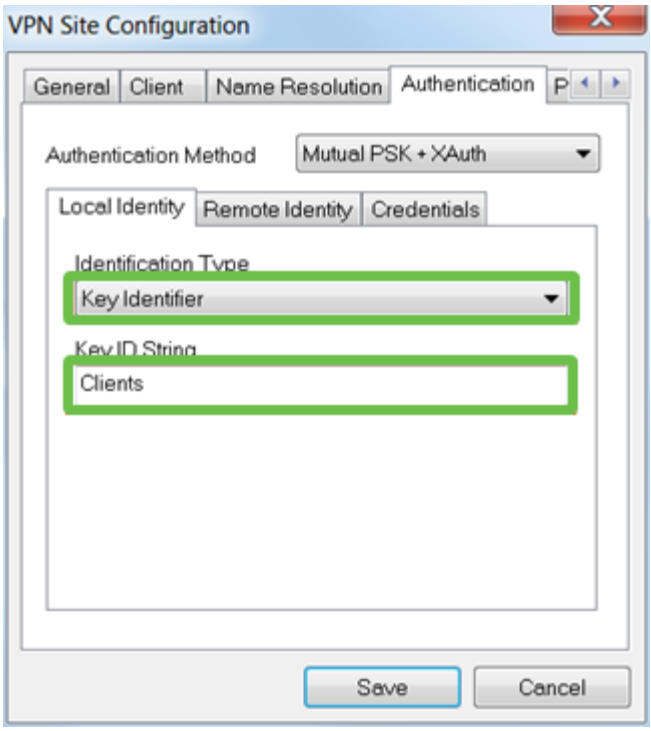
Na guia **Name Resolution > WINS**, marque a caixa **Enable WINS** e deixe a caixa **Obtain Automatically (Obter automaticamente)** marcada.



Etapa 5

Clique em **Authentication > Local Identity**.

- **Tipo de identificação**: Selecionar **Identificador de Chave**
- **String de ID da Chave**: Insira o **nome do grupo** configurado no RV345P

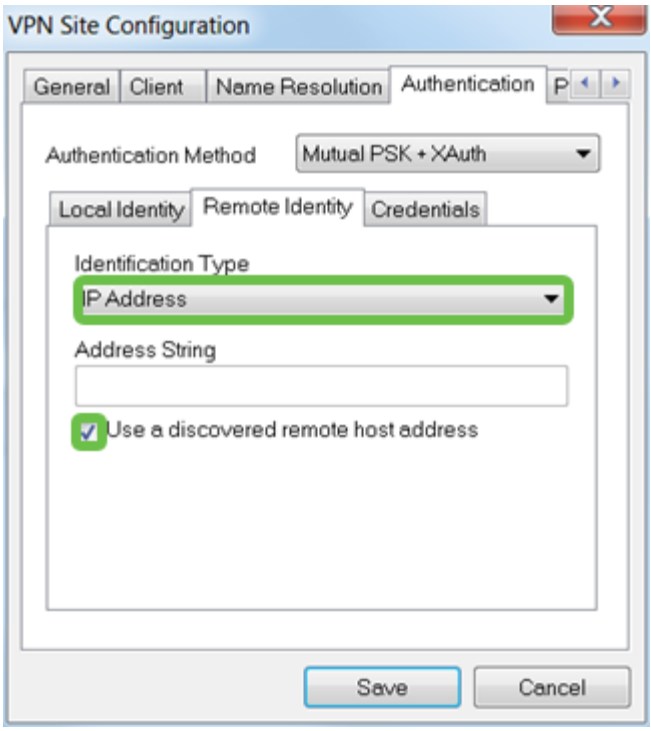


Etapa 6

Em **Authentication > Remote Identity**. Neste exemplo, mantivemos as configurações

padrão.

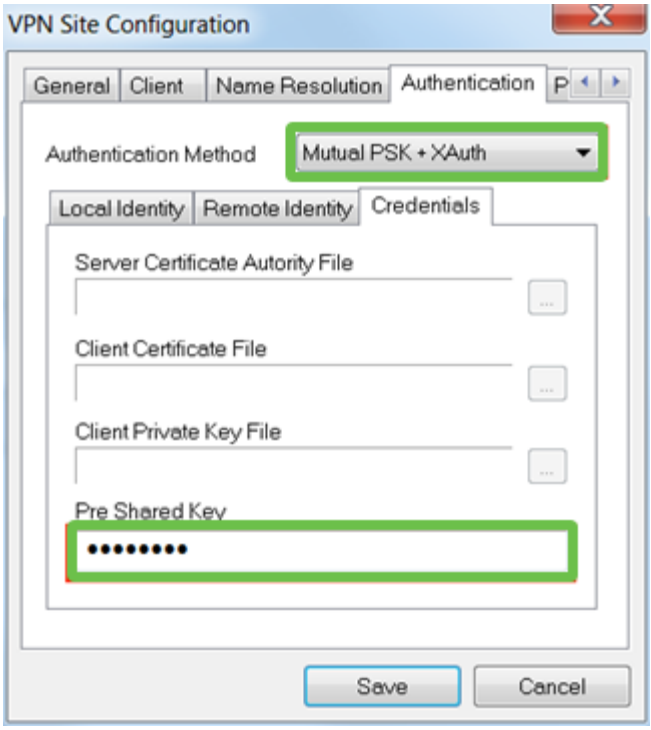
- **Tipo de identificação**: IP Address
- **String de Endereço**: <blank>
- **Use uma** caixa **de endereço de host remoto descoberta**: Verificado



Etapa 7

Em **Authentication > Credentials**, configure o seguinte:

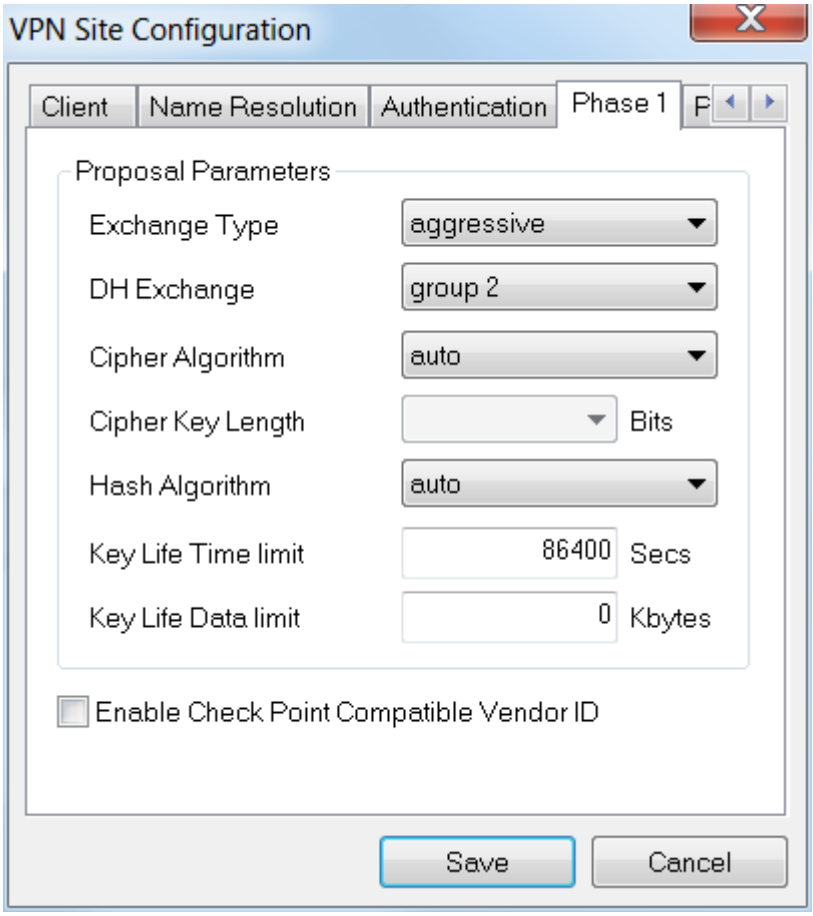
- **método de autenticação:** Selecione **PSK Mútua + XAuth**
- **Chave pré-compartilhada**: Insira a **chave pré-compartilhada** configurada no perfil do cliente RV345P



Passo 8

Para a guia **Fase 1**. Neste exemplo, as configurações padrão foram mantidas:

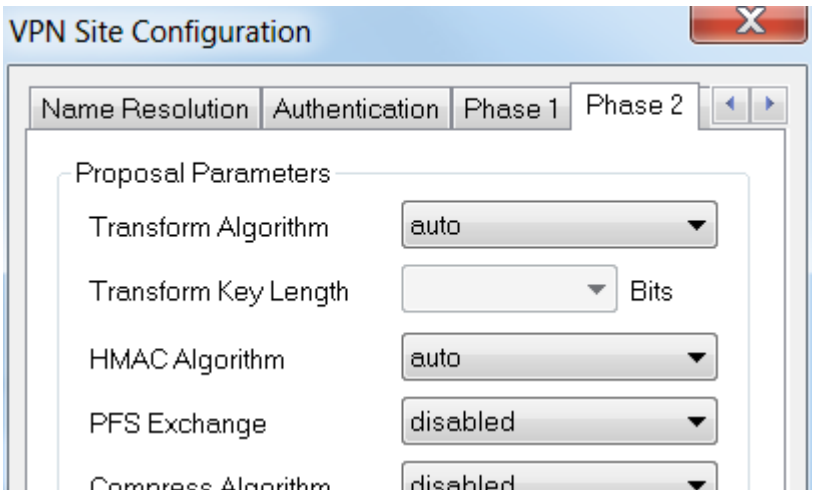
- **Tipo de Troca:** Agressivo
- **DH Exchange:** grupo 2
- **Algoritmo de cifra:** Automático
- **Algoritmo de hash:** Automático



Passo 9

Neste exemplo, os padrões para a guia **Fase 2** foram mantidos iguais.

- **Algoritmo de transformação:** Automático
- **Algoritmo HMAC:** Automático
- **PFS Exchange:** Desabilitado
- **Compactar algoritmo:** desabilitado

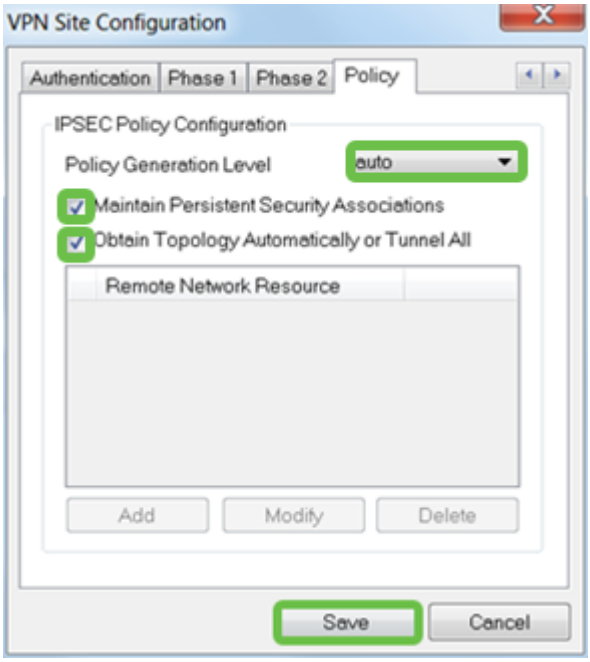


Passo 10

Para o exemplo da guia **Política**, usamos as seguintes configurações:

- **Nível de geração de política:** Automático
- **Manter associações de segurança persistentes:** verificado
- **Obter Topologia Automaticamente ou Túnel Tudo:** Verificado

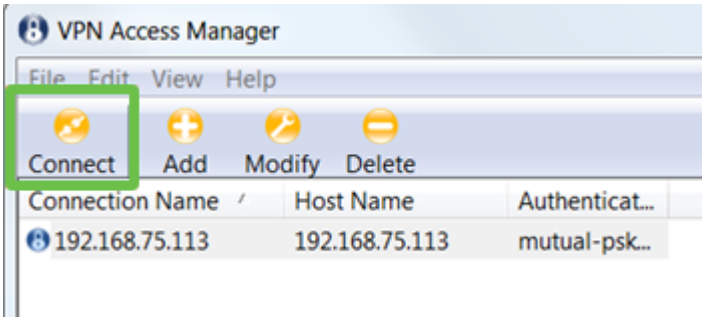
Como configuramos **Split-Tunneling** no RV345P, não precisamos configurá-lo aqui.



Ao concluir, clique em Save (Salvar).

Passo 11

Agora você está pronto para testar a conexão. No *VPN Access Manager*, realce o perfil de conexão e clique no botão **Connect**.

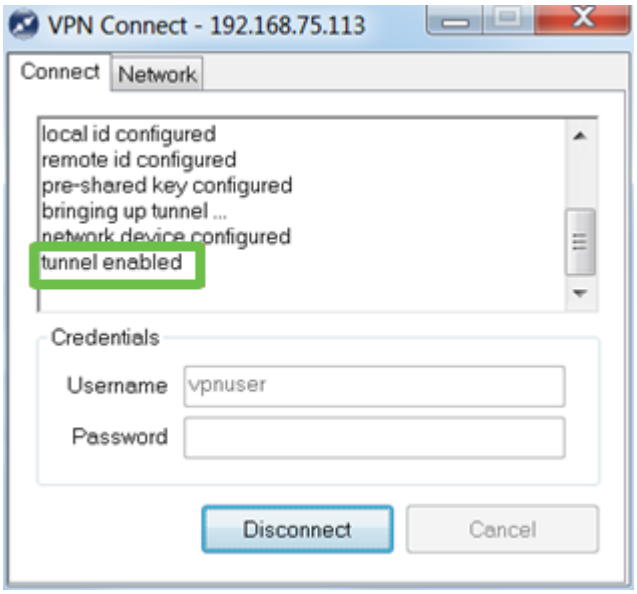


Etapa 12

Na janela **VPN Connect** exibida, insira o **Nome de usuário** e a **Senha** usando as credenciais da **conta de usuário** criada no RV345P (etapas 13 e 14). Quando terminar, clique em **Connect**.

Passo 13

Verifique se o túnel está conectado. Você deve ver o **túnel ativado**.



O Shrew Soft foi usado como exemplo nesta configuração. Como a Shrew Soft não é um produto da Cisco, entre em contato com esse terceiro caso precise de assistência técnica.

Outras opções de VPN

Há outras opções para o uso de uma VPN. Clique nos links a seguir para obter mais informações:

- Usar o GreenBow VPN Client para se conectar ao RV34x Series Router
- Configurar um cliente de VPN de trabalhador remoto no roteador RV34x Series
- Configurar um servidor PPTP (Point-to-Point Tunneling Protocol) no roteador Rv34x Series
- Configurar um perfil de segurança de protocolo Internet (IPsec) em um roteador RV34x Series

- Configurar L2TP WAN no roteador RV34x
- Configuração de VPN site a site no RV34x

Configurações suplementares no roteador RV345P

Configurar VLANs (opcional)

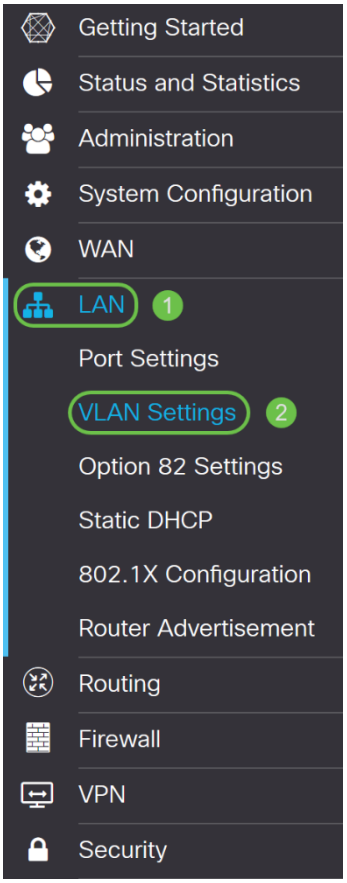
Uma rede local virtual (VLAN) permite segmentar logicamente uma rede de área local (LAN) em diferentes domínios de transmissão. Nos cenários em que dados confidenciais podem ser transmitidos em uma rede, as VLANs podem ser criadas para aumentar a segurança, designando uma transmissão para uma VLAN específica. As VLANs também podem ser usadas para melhorar o desempenho, reduzindo a necessidade de enviar broadcasts e multicasts para destinos desnecessários. Você pode criar uma VLAN, mas isso não tem efeito até que a VLAN seja conectada a pelo menos uma porta, manual ou dinamicamente. As portas devem sempre pertencer a uma ou mais VLANs.

Consulte as Melhores práticas de VLAN e as Dicas de segurança para obter mais orientações.

Se não quiser criar VLANs, você pode ir para a próxima seção.

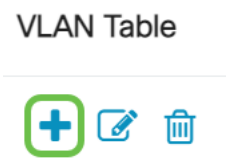
Passo 1

Navegue até **LAN > VLAN Settings**.



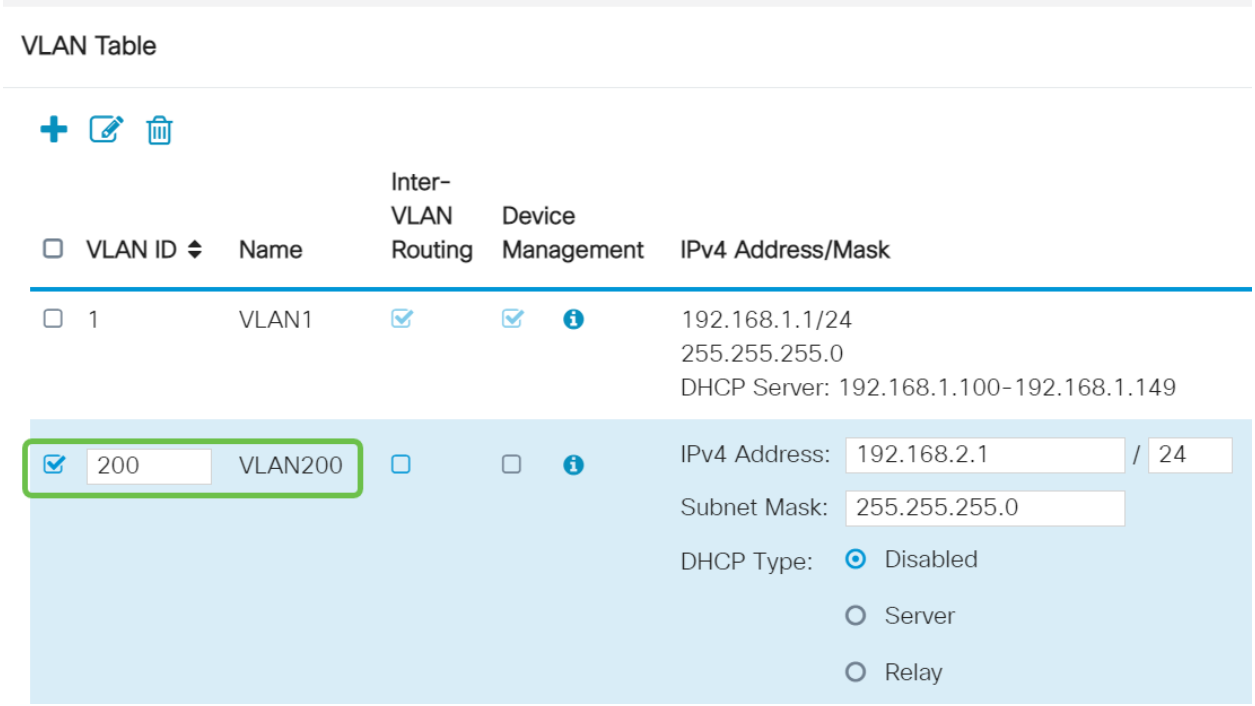
Passo 2

Clique no **ícone Adicionar** para criar uma nova VLAN.



Etapa 3

Digite o *ID da VLAN* que deseja criar e um *Nome* para ele. O intervalo de *ID* da *VLAN* é de 1 a 4093.



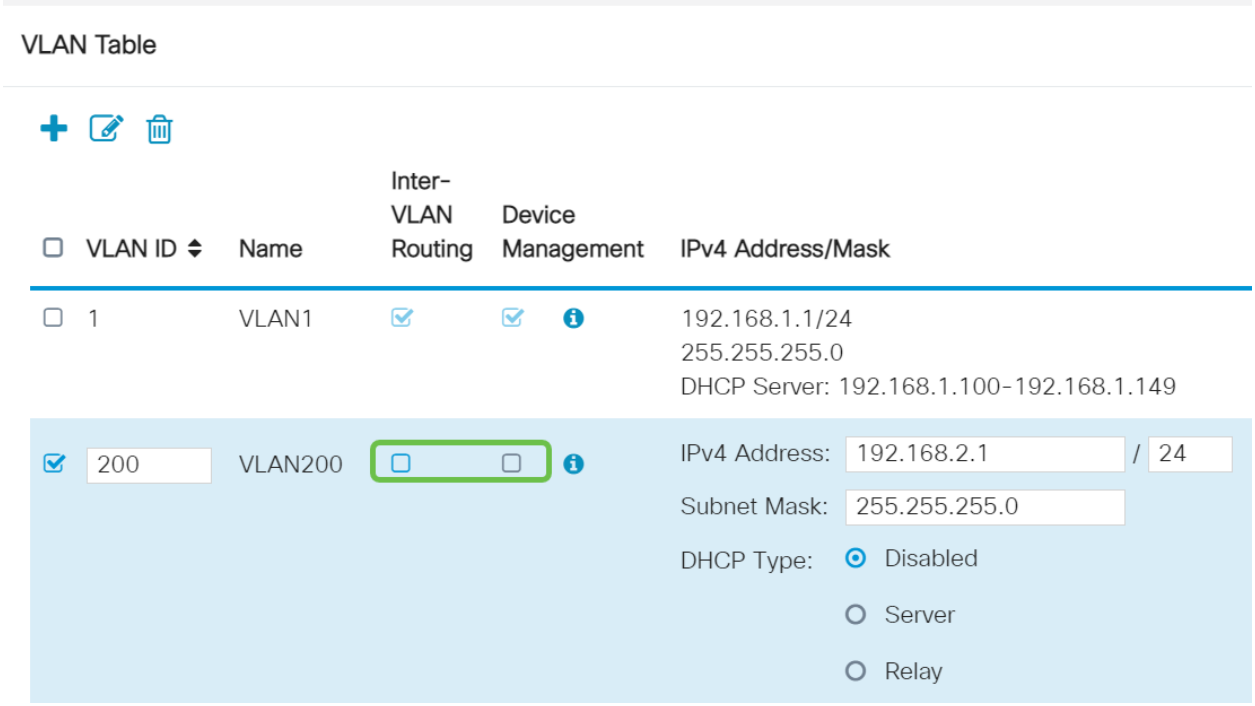
Passo 4

Desmarque a caixa *Habilitado* para *Roteamento entre VLANs* e *Gerenciamento de dispositivos* se desejar. O roteamento entre VLANs é usado para rotear pacotes de uma VLAN para outra VLAN.

Em geral, isso não é recomendado para redes de convidados, pois você vai querer isolar os usuários convidados, deixando as VLANs menos seguras. Às vezes, pode ser necessário que as VLANs façam o roteamento entre si. Se for esse o caso, verifique o Roteamento entre VLANs em um roteador RV34x com restrições de ACL direcionadas para configurar o tráfego específico que você permite entre VLANs.

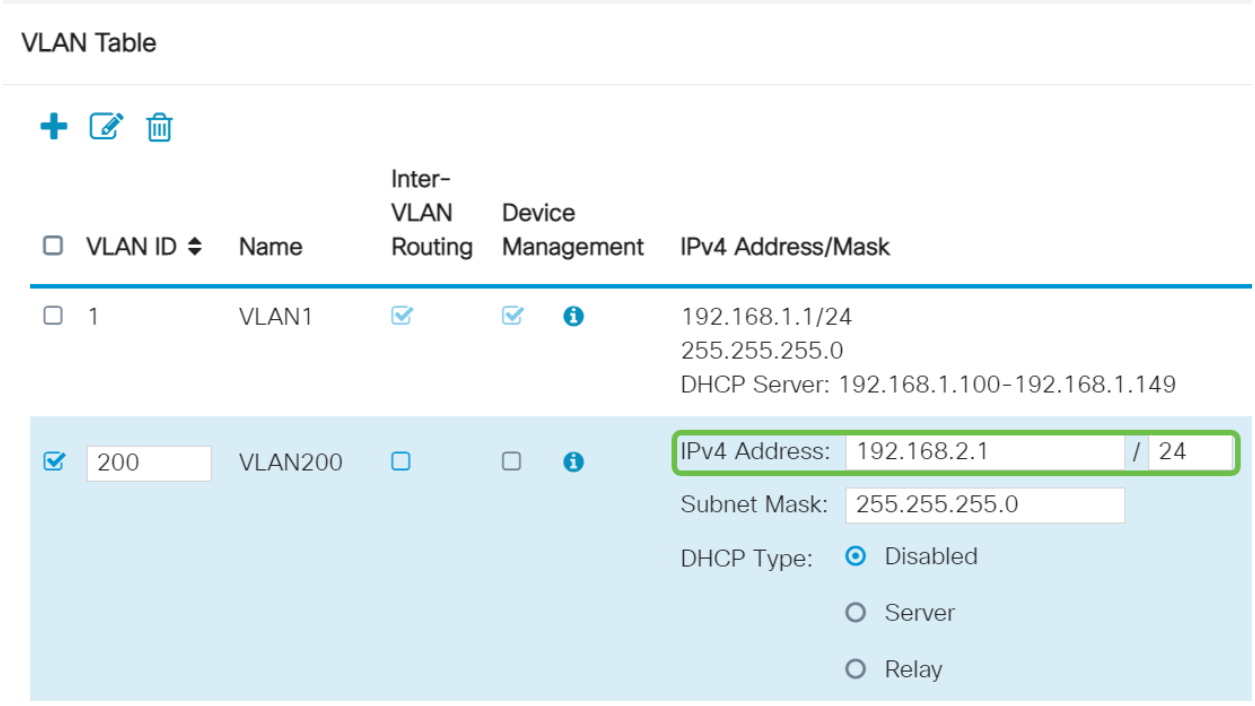
O Gerenciamento de dispositivos é o software que permite usar o navegador para fazer login na IU da Web do RV345P, a partir da VLAN, e gerenciar o RV345P. Isso também deve ser desativado em redes de Convidados.

Neste exemplo, não habilitamos o *roteamento entre VLANs* ou o *gerenciamento de dispositivos* para manter a VLAN mais segura.



Etapa 5

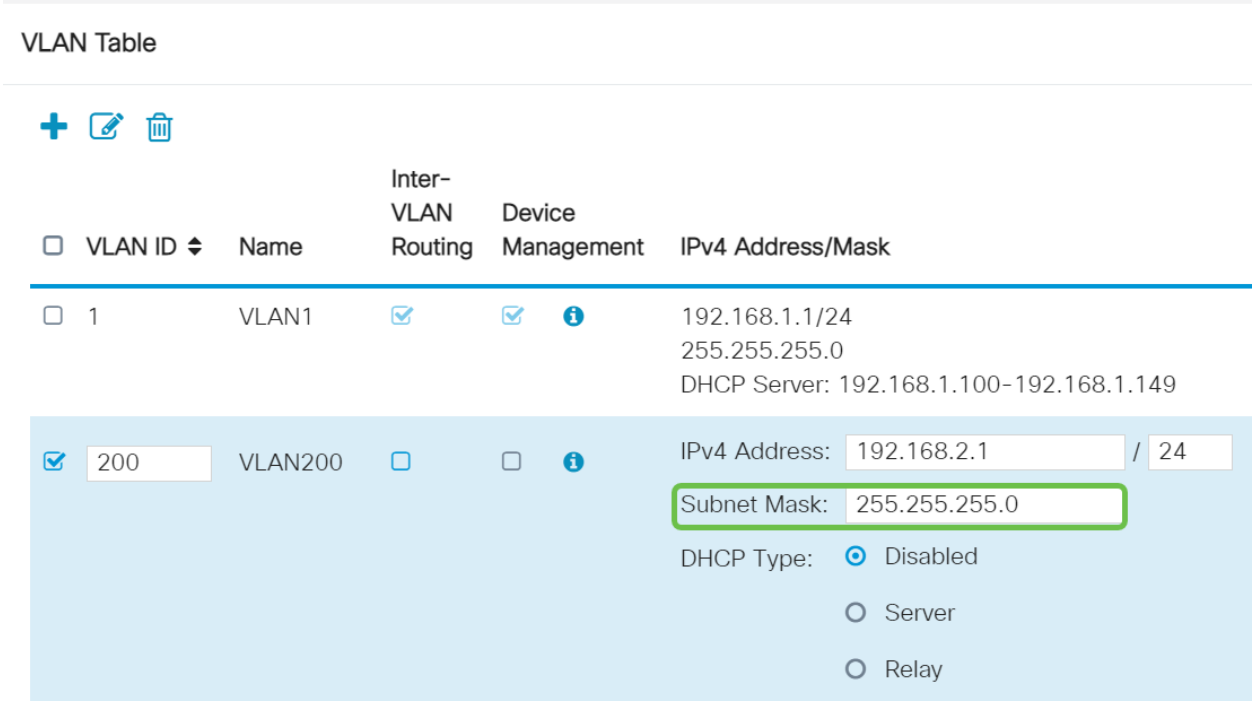
O endereço IPv4 privado será preenchido automaticamente no campo *Endereço IP*. Você pode ajustar isso se escolher. Neste exemplo, a sub-rede tem endereços IP 192.168.2.100-192.168.2.149 disponíveis para DHCP. 192.168.2.1-192.168.2.99 e 192.168.2.150-192.168.2.254 estão disponíveis para endereços IP estáticos.



Etapa 6

A máscara de sub-rede em *Máscara de sub-rede* será preenchida automaticamente. Se você fizer alterações, o campo será automaticamente ajustado.

Para esta demonstração, deixaremos a *Máscara de sub-rede* como **255.255.255.0** ou **/24**.



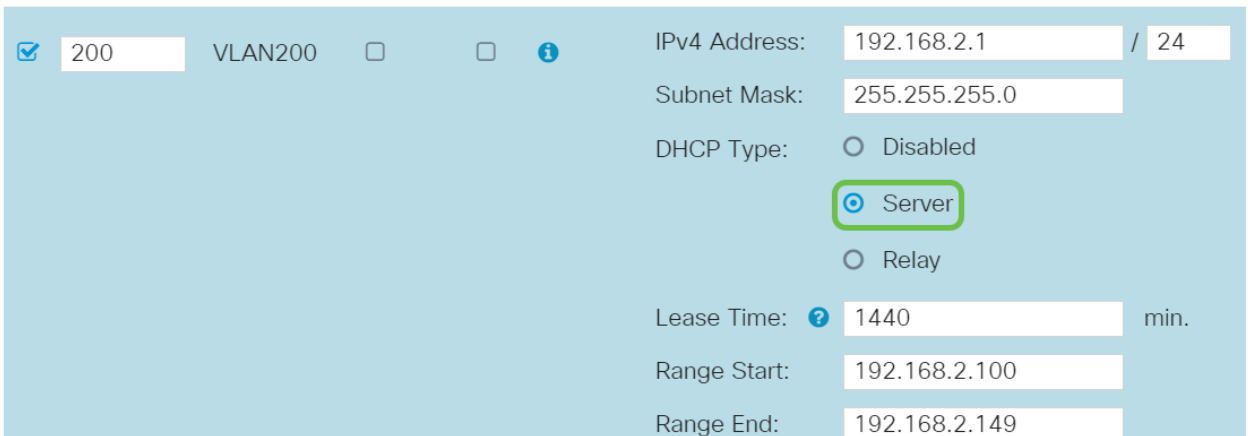
Etapa 7

Selecione um *tipo de protocolo DHCP*. As seguintes opções são:

Disabled (Desabilitado) - Desabilita o servidor DHCP IPv4 na VLAN. Isso é recomendado em um ambiente de teste. Nesse cenário, todos os endereços IP precisariam ser configurados manualmente e toda a comunicação seria interna.

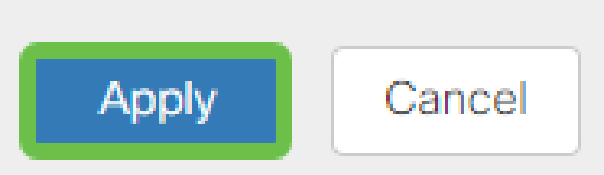
Server - Esta é a opção mais usada.

- Tempo de concessão - Insira um valor de tempo de 5 a 43.200 minutos. O padrão é 1440 minutos (igual a 24 horas).
- Intervalo Início e Intervalo Final - Insira o intervalo de início e fim dos endereços IP que podem ser atribuídos dinamicamente.
- Servidor DNS - Selecione para usar o servidor DNS como proxy ou do ISP na lista suspensa.
- WINS Server - Insira o nome do servidor WINS.
- Opções de DHCP:
    - Opção 66 - Insira o endereço IP do servidor TFTP.
    - Opção 150 - Insira o endereço IP de uma lista de servidores TFTP.
    - Opção 67 - Insira o nome do arquivo de configuração.
- Relay - Insira o endereço IPv4 do servidor DHCP remoto para configurar o agente de retransmissão DHCP. Essa é uma configuração mais avançada.



Passo 8

Clique em **Apply** para criar a nova VLAN.



Atribuir VLANs às portas (opcional)

16 VLANs podem ser configuradas no RV345P, com uma VLAN para a rede de longa distância (WAN). As VLANs que não estão em uma porta devem ser *excluídas*. Isso mantém o tráfego nessa porta exclusivamente para as VLAN/VLANs especificamente atribuídas pelo usuário. É considerada uma boa prática.

As portas podem ser definidas como uma porta de acesso ou uma porta de tronco:

- Porta de acesso - uma VLAN atribuída. Os quadros não marcados são passados.
- Porta de tronco - Pode transportar mais de uma VLAN. 802.1q. o entroncamento permite que uma VLAN nativa seja desmarcada. As VLANs que você não deseja no tronco devem ser excluídas.

Uma VLAN atribuiu sua própria porta:

- Considerada uma porta de acesso.
- A VLAN atribuída a esta porta deve ser rotulada como Não rotulada.
- Todas as outras VLANs devem ser rotuladas como Excluídas para essa porta.

Duas ou mais VLANs que compartilham uma porta:

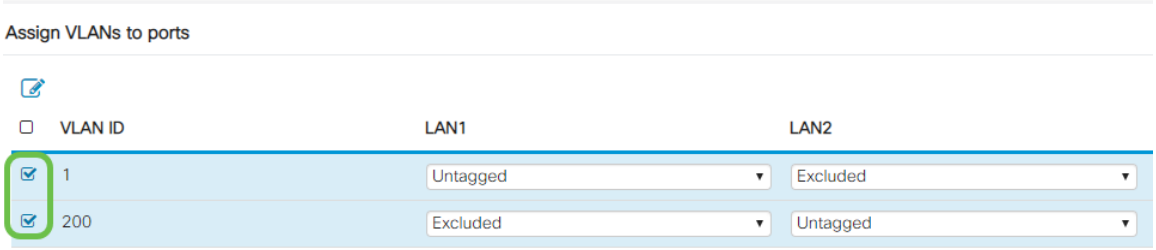
- Considerada uma porta de tronco.
- Uma das VLANs pode ser rotulada como Não rotulada.
- O restante das VLANs que fazem parte da porta de tronco deve ser rotulado como Marcado.
- As VLANs que não fazem parte da Porta de Tronco devem ser rotuladas Excluídas para essa porta.

Neste exemplo, não há troncos.

Passo 1

Selecione as *IDs de VLAN* a serem editadas.

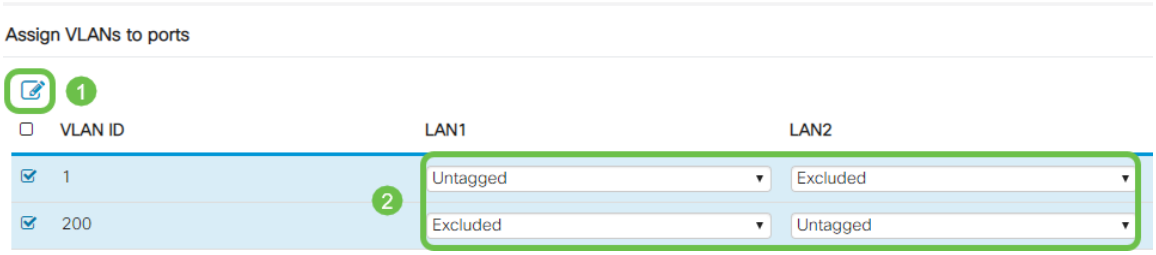
Neste exemplo, selecionamos *VLAN 1* e *VLAN 200*.



Passo 2

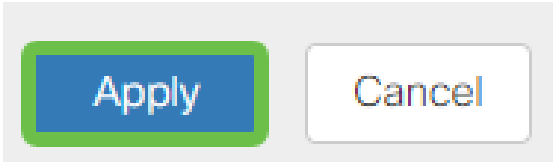
Clique em **Editar** para atribuir uma VLAN a uma porta LAN e especifique cada configuração como *Marcada*, *Não Marcada* ou *Excluída*.

Neste exemplo, em LAN1, atribuímos a VLAN 1 como **Não Marcada** e a VLAN 200 como **Excluída**. Para LAN2, atribuímos a VLAN 1 como **excluída** e a VLAN 200 como **não rotulada**.



Etapa 3

Clique em **Apply** para salvar a configuração.



Agora você deve ter criado com êxito uma nova VLAN e configurado VLANs para portas no RV345P. Repita o processo para criar as outras VLANs. Por exemplo, a VLAN300 seria criada para o Marketing com uma sub-rede de 192.168.3.x e a VLAN400 seria criada para o Accounting com uma sub-rede de 192.168.4.x.

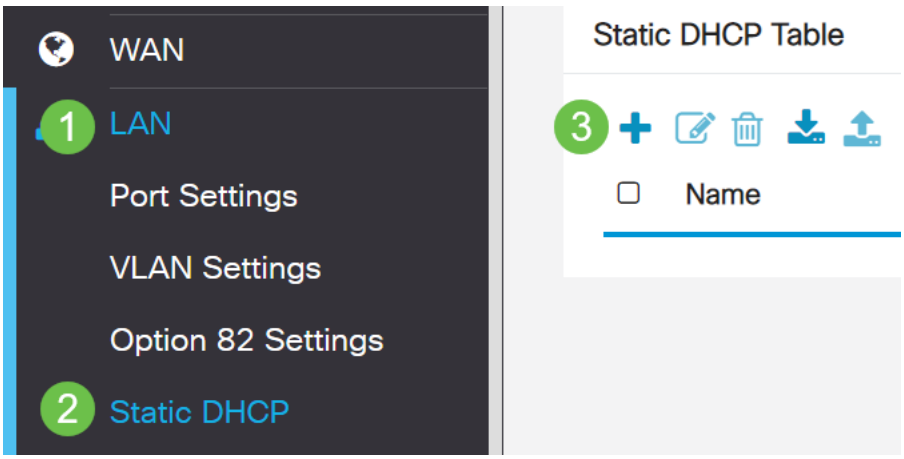
Adicionar um IP estático (opcional)

Se você quiser que um determinado dispositivo esteja acessível a outras VLANs, você pode dar a esse dispositivo um endereço IP local estático e criar uma regra de acesso para torná-lo acessível. Isso só funciona se o roteamento entre VLANs estiver ativado. Há outras situações em que um IP estático pode ser útil. Para obter mais informações sobre como configurar endereços IP estáticos, consulte Práticas recomendadas para configurar endereços IP estáticos no hardware comercial da Cisco.

Se não precisar adicionar um endereço IP estático, você pode ir para a próxima seção deste artigo.

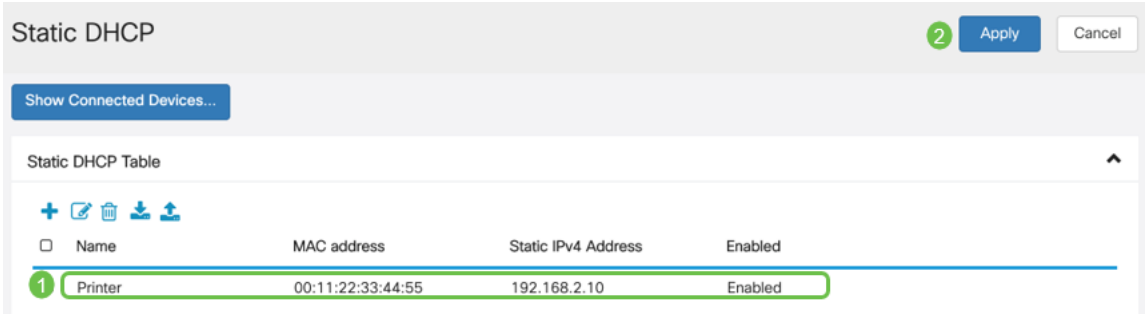
Passo 1

Navegue até **LAN > DHCP estático.** Clique no **ícone de mais**.



Passo 2

Adicione as informações **DHCP estático** para o dispositivo. Neste exemplo, o dispositivo é uma impressora.



Gerenciamento de certificados (opcional)

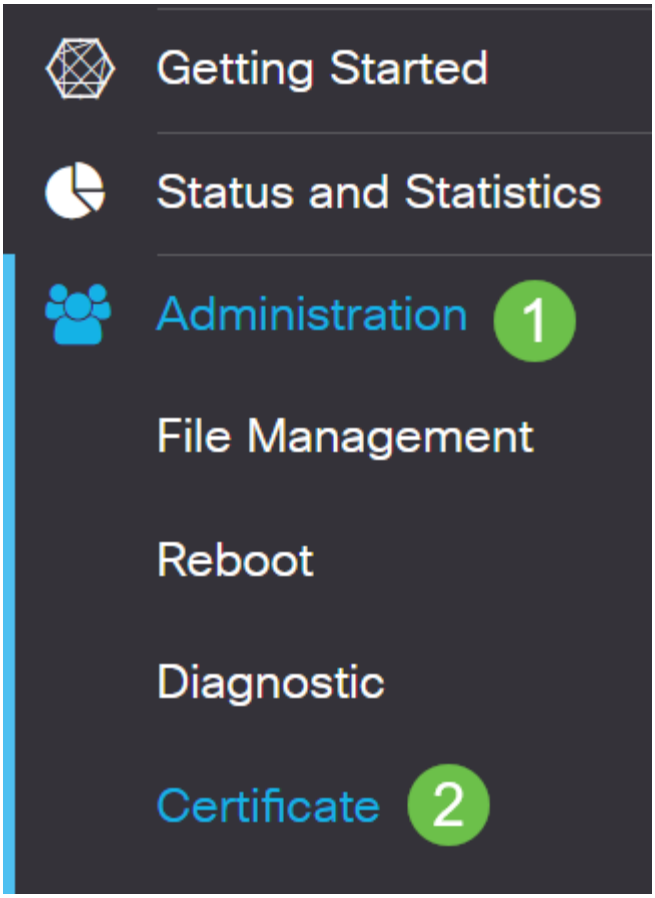
Um certificado digital certifica a propriedade de uma chave pública pelo assunto nomeado do certificado. Isso permite que as partes confiáveis dependam de assinaturas ou asserções feitas pela chave privada que corresponda à chave pública certificada. Um roteador pode gerar um certificado autoassinado, um certificado criado por um administrador de rede. Pode também enviar pedidos às Autoridades de Certificação (AC) para solicitarem um certificado de identidade digital. É importante ter certificados legítimos de aplicativos de terceiros.

Uma autoridade de certificação (AC) é usada para autenticação. Os certificados podem ser adquiridos de qualquer número de sites de terceiros. É uma forma oficial de provar que seu site é seguro. Essencialmente, a AC é uma fonte confiável que verifica se você é uma empresa legítima e se pode ser confiável. Dependendo das suas necessidades, um certificado a um custo mínimo. Você recebe check-out do CA e, depois que ele verificar suas informações, ele emitirá o certificado para você. Este certificado pode ser baixado como um arquivo em seu computador. Você pode então ir para o roteador (ou servidor VPN) e carregá-lo lá.

Gerar CSR/certificado

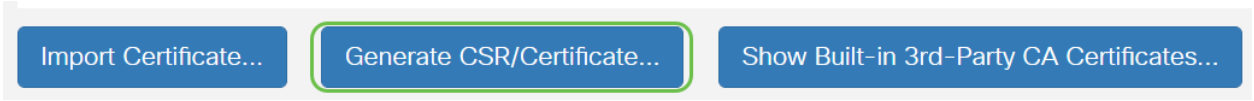
Passo 1

Faça login no utilitário baseado na Web do roteador e escolha **Administration > Certificate**.



Passo 2

Clique em **Gerar CSR/Certificado**. Você será direcionado para a página Gerar CSR/Certificado.



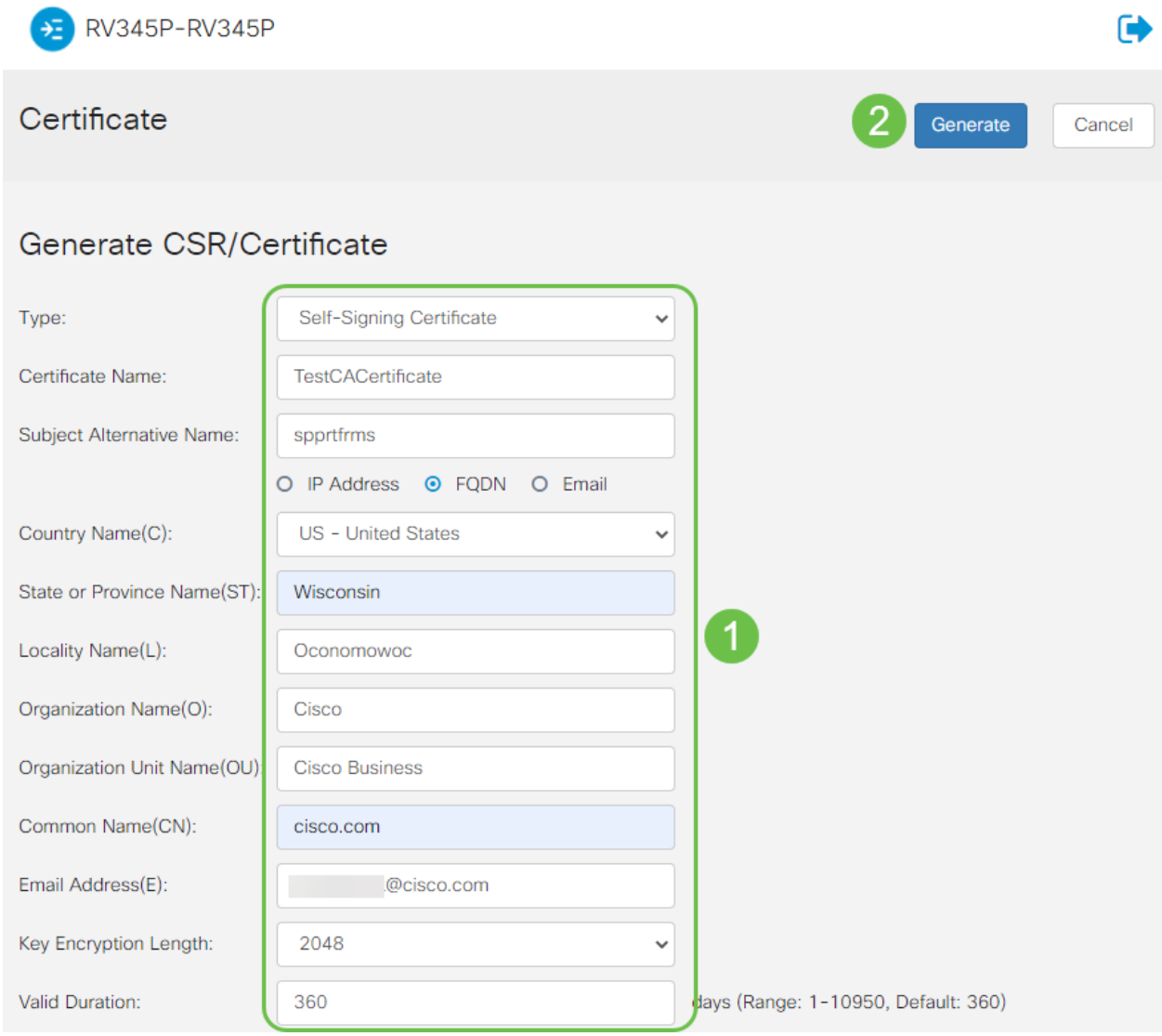
Etapa 3

Preencha as caixas com o seguinte:

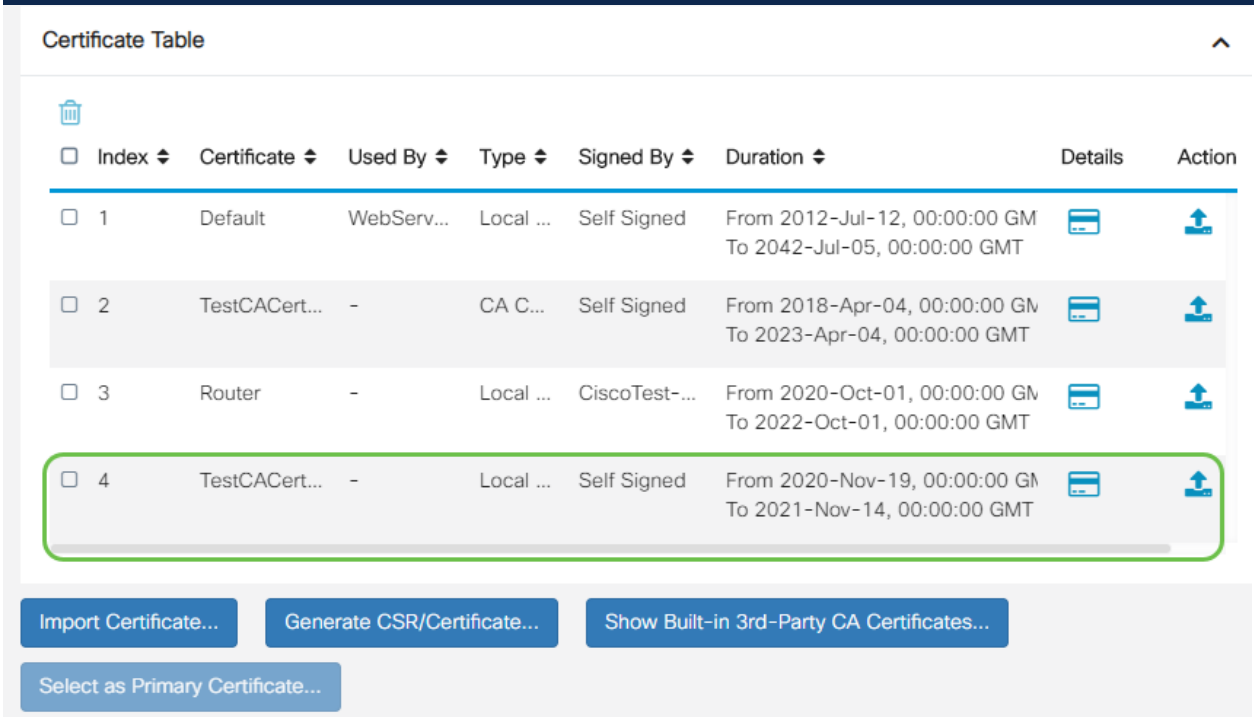
- Escolha o tipo de certificado apropriado
  - Certificado de assinatura automática — Este é um certificado SSL (Secure Socket Layer) assinado por seu próprio criador. Este certificado é menos confiável, pois não pode ser cancelado se a chave privada for comprometida de alguma forma por um invasor.
  - Solicitação de assinatura certificada — esta é uma infraestrutura de chave pública (PKI) que é enviada à autoridade de certificação para solicitar um certificado de identidade digital. É mais segura do que autoassinada, já que a chave privada é mantida em segredo.
- Insira um nome para seu certificado no campo Nome do certificado para identificar a solicitação. Este campo não pode estar em branco nem conter espaços e caracteres especiais.
- (Opcional) Na área Nome alternativo do assunto, clique em um botão de opção. As opções são:
  - Endereço IP — Insira um endereço IP (Internet Protocol [protocolo de

Internet])
    - FQDN — Insira um nome de domínio totalmente qualificado (FQDN)
    - E-mail — insira um endereço de e-mail

- No campo Nome alternativo do assunto, insira o FQDN.
- Escolha um nome de país no qual sua organização está legalmente registrada na lista suspensa Nome do país.
- Insira um nome ou uma abreviação do estado, província, região ou território onde sua organização está localizada no campo Estado ou Nome da província (ST).
- Insira um nome da localidade ou cidade em que sua organização está registrada ou localizada no campo Nome da localidade.
- Insira um nome com o qual sua empresa está legalmente registrada. Se você estiver se inscrevendo como uma pequena empresa ou como um único proprietário, insira o nome do solicitante de certificado no campo Nome da empresa. Não é possível usar caracteres especiais.
- Insira um nome no campo Nome da unidade da organização para diferenciar divisões dentro de uma organização.
- Digite um nome no campo Nome comum. Esse nome deve ser o nome de domínio totalmente qualificado do site para o qual você usa o certificado.
- Insira o endereço de e-mail da pessoa que deseja gerar o certificado.
- Na lista suspensa Tamanho da criptografia de chave, escolha um comprimento de chave. As opções são 512, 1024 e 2048. Quanto maior o comprimento da chave, mais seguro o certificado.
- No campo Duração válida, insira o número de dias em que o certificado será válido. O padrão é 360.
- Clique em **Gerar**.



O certificado gerado agora deve aparecer na Tabela de certificados.

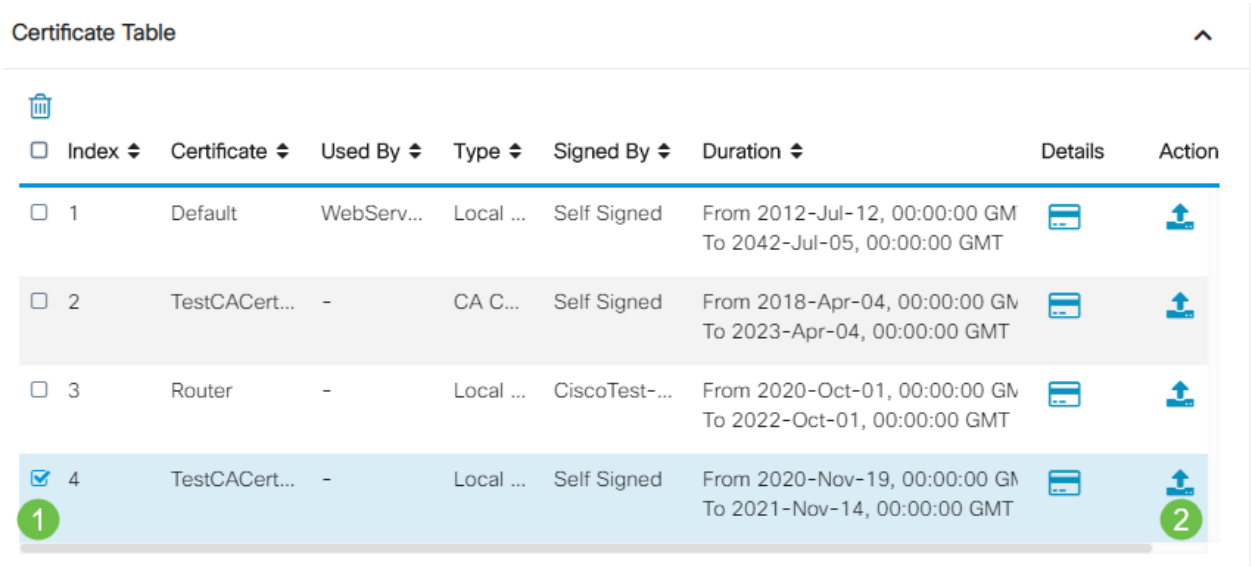


Agora você deve ter criado com êxito um certificado no roteador RV345P.

Exportar um certificado

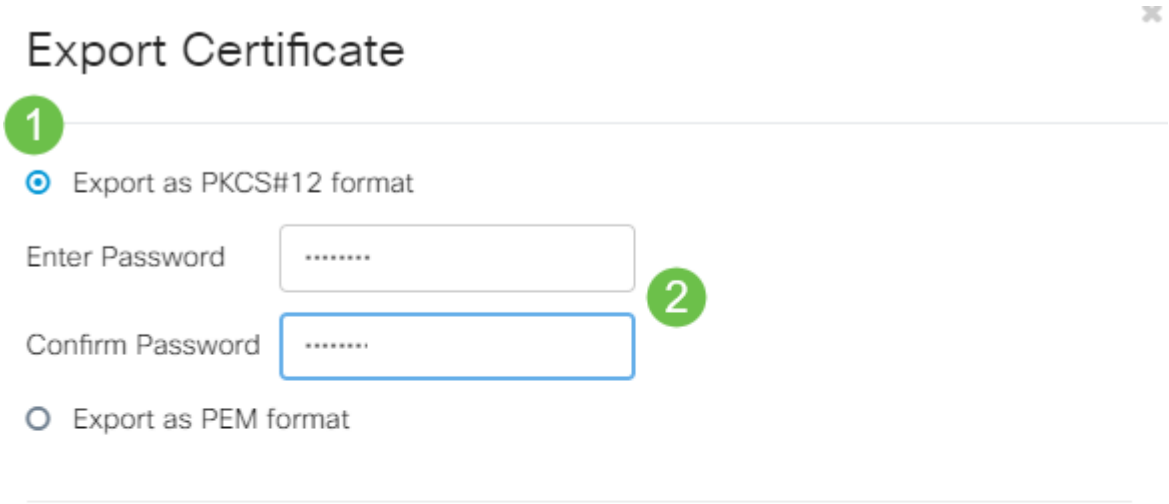
Passo 1

Na Tabela de certificados, marque a caixa de seleção do certificado que deseja exportar e clique no **ícone exportar**.



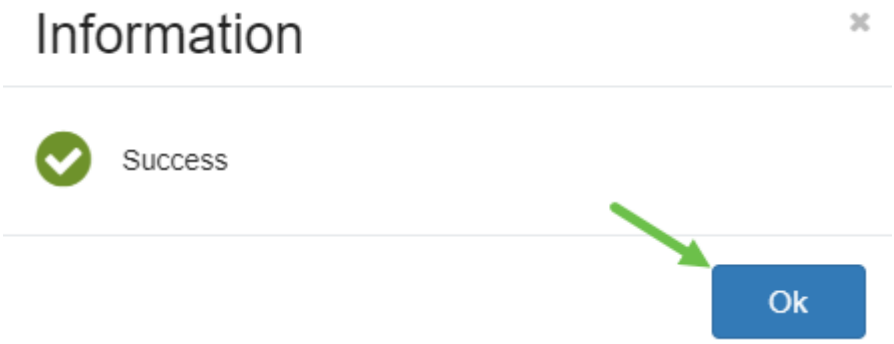
Passo 2

- Clique em um formato para exportar o certificado. As opções são:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 é um certificado exportado que vem em uma extensão .p12. Será necessária uma senha para criptografar o arquivo para protegê-lo à medida que for exportado, importado e excluído.
  - PEM — O Privacy Enhanced Mail (PEM) é frequentemente usado para servidores Web para que eles possam ser facilmente traduzidos em dados legíveis usando um editor de texto simples, como o notepad.
- Se você escolheu PEM, clique em **Exportar**.
- Insira uma senha para proteger o arquivo a ser exportado no campo Inserir senha.
- Digite novamente a senha no campo Confirmar senha.
- Na área Selecionar destino, o PC foi escolhido e é a única opção disponível no momento.
- Clique em **Exportar**.



Etapa 3

Uma mensagem indicando o sucesso do download será exibida abaixo do botão Download. Um arquivo começará a ser baixado em seu navegador. Click OK.

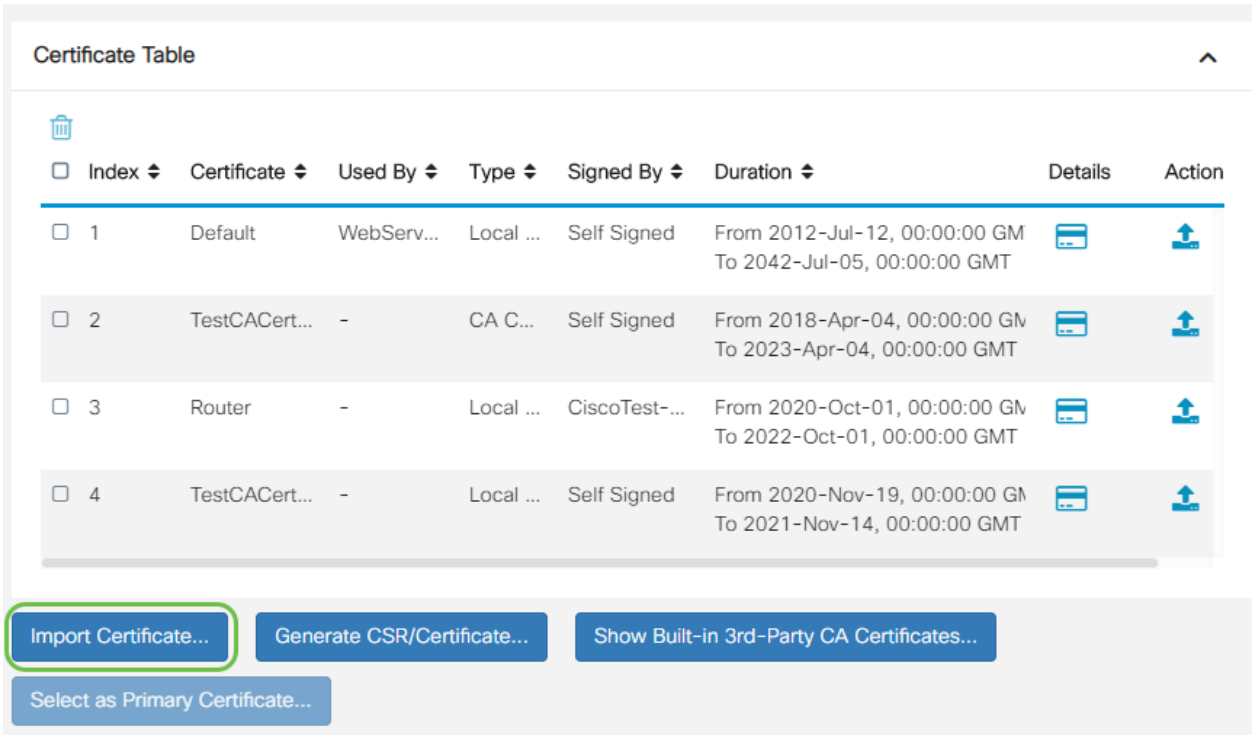


Você deve ter exportado com êxito um certificado no RV345P Series Router.

Importar um certificado

Passo 1

Clique em **Importar certificado...**.

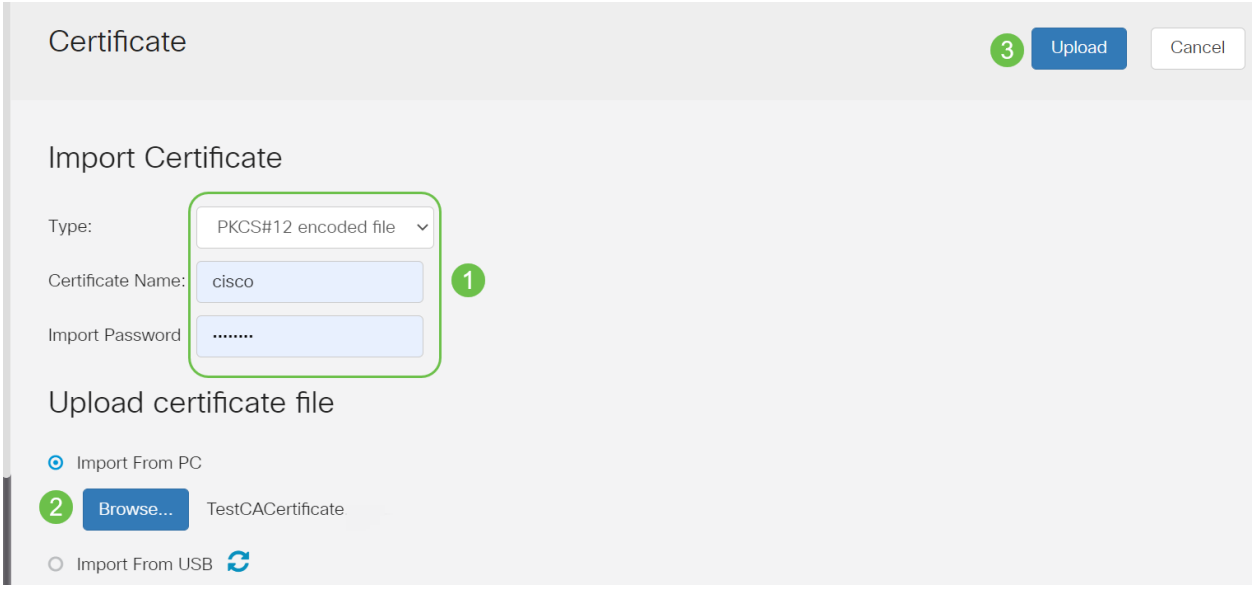


Passo 2

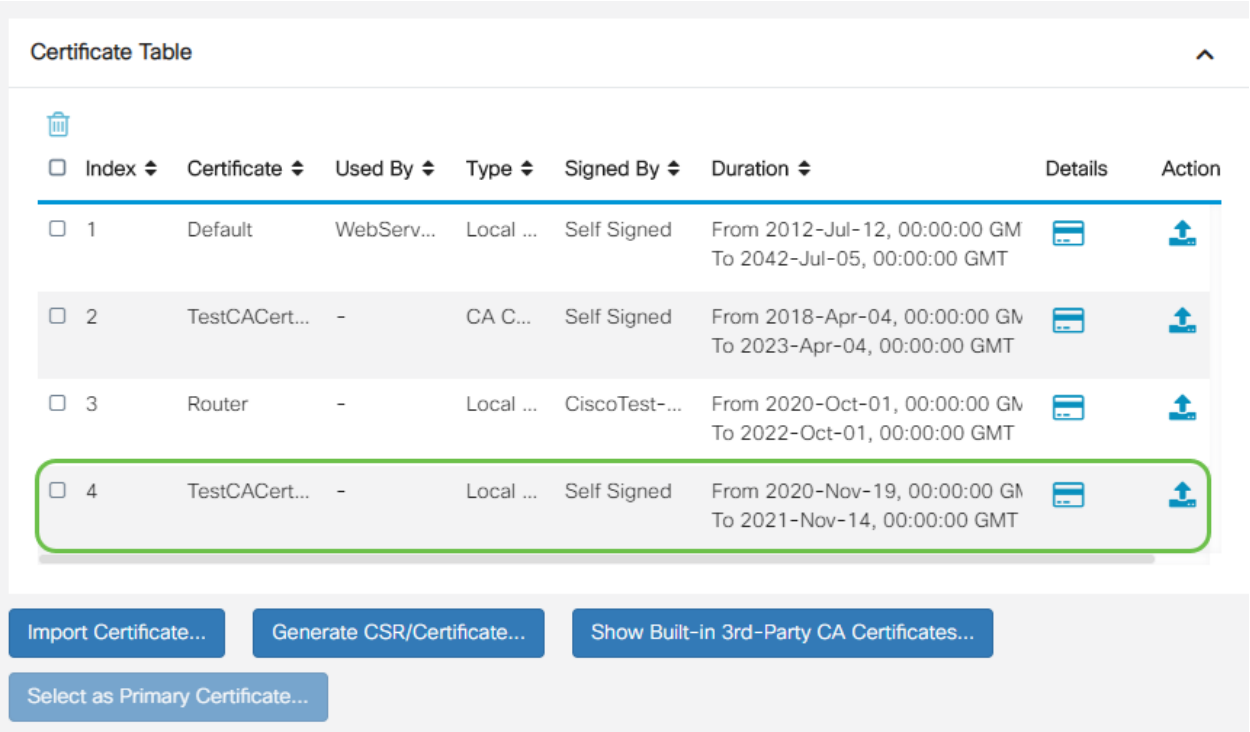
- Escolha o tipo de certificado a importar na lista suspensa. As opções são:
  - Certificado local — Um certificado gerado no roteador.
  - Certificado CA — Um certificado certificado certificado certificado por uma autoridade de terceiros confiável que confirmou a exatidão das informações contidas no certificado.
  - Arquivo codificado PKCS #12 — PKCS #12 é um formato de armazenamento de um certificado de servidor.

- Insira um nome para o certificado no campo Nome do certificado.
- Se PKCS #12 foi escolhido, insira uma senha para o arquivo no campo Import Password (Importar senha). Caso contrário, vá para o passo 3.
- Clique em uma origem para importar o certificado. As opções são:
    - Importar do PC
    - Importar de USB

- Se o roteador não detectar uma unidade USB, a opção Import from USB (Importar de USB) ficará acinzentada.
- Se você escolheu Importar de USB e seu USB não está sendo reconhecido pelo roteador, clique em Atualizar.
- Clique no botão Escolher arquivo e escolha o arquivo apropriado.
- Clique em Fazer upload.



Depois de obter êxito, você será automaticamente levado para a página principal Certificado. A tabela de certificados será preenchida com o certificado importado recentemente.



Você deve ter importado com êxito um certificado no roteador RV345P.

Configurar uma rede móvel usando um dongle e um roteador RV345P Series (opcional)

Talvez você queira configurar uma rede móvel de backup usando um dongle e seu roteador RV345P. Se esse for o caso, você deve ler Configure a rede móvel usando um dongle e um roteador RV34x Series.

Parabéns, você concluiu a configuração do roteador RV345P! Agora você configurará seus dispositivos sem fio comerciais da Cisco.

Configurar o CBW140AC

CBW140AC pronto para uso

Comece conectando um cabo Ethernet da porta PoE no CBW140AC a uma porta PoE no RV345P. As primeiras 4 portas no RV345P podem fornecer PoE, para que qualquer uma delas possa ser usada.

Verifique o status das luzes indicadoras. O ponto de acesso levará cerca de 10 minutos para ser inicializado. O LED piscará em verde em vários padrões, alternando rapidamente entre verde, vermelho e âmbar antes de ficar verde novamente. Pode haver pequenas variações na intensidade da cor do LED e na tonalidade de unidade para unidade. Quando a luz do LED estiver piscando em verde, vá para a próxima etapa.

A porta de uplink Ethernet PoE no AP primário SÓ pode ser usada para fornecer um uplink para a LAN e NÃO para se conectar a qualquer outro dispositivo de extensor de malha ou com capacidade primária.

Se o seu ponto de acesso não for novo, verifique se ele está redefinido para as configurações padrão de fábrica do SSID *Cisco Business-Setup* para aparecer em suas opções Wi-Fi. Para obter ajuda com isso, consulte Como reinicializar e redefinir as configurações padrão de fábrica nos roteadores RV345x.

Configurar o ponto de acesso sem fio principal 140AC na interface do usuário da Web

Você pode configurar o ponto de acesso usando o aplicativo móvel ou a interface de usuário da Web. Este artigo usa a interface de usuário da Web para configuração, que oferece mais opções para configuração, mas é um pouco mais complicada. Se quiser usar o aplicativo móvel para as próximas seções, clique para acessar as instruções do aplicativo móvel.

Se tiver problemas para se conectar, consulte a seção Dicas de solução de problemas sem fio deste artigo.

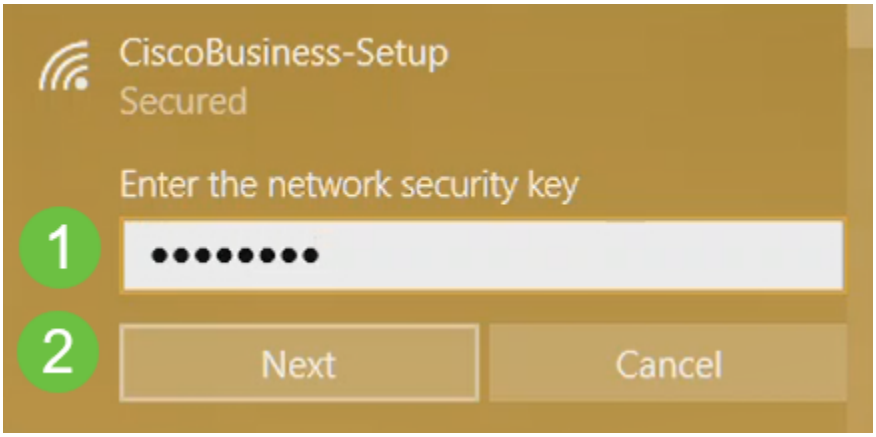
Passo 1

No PC, clique no **ícone Wi-Fi** e escolha rede sem fio *Cisco Business-Setup*. Clique em Conectar.

Se o seu ponto de acesso não for novo, verifique se ele está redefinido para as configurações padrão de fábrica do SSID *Cisco Business-Setup* para aparecer em suas opções Wi-Fi.

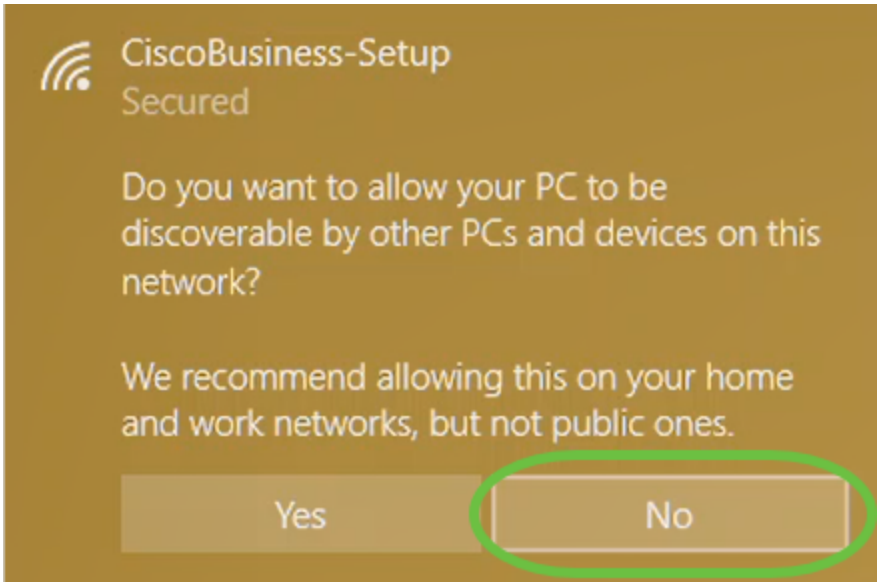
Passo 2

Insira a senha **cisco123** e clique em **Avançar**.



Etapa 3

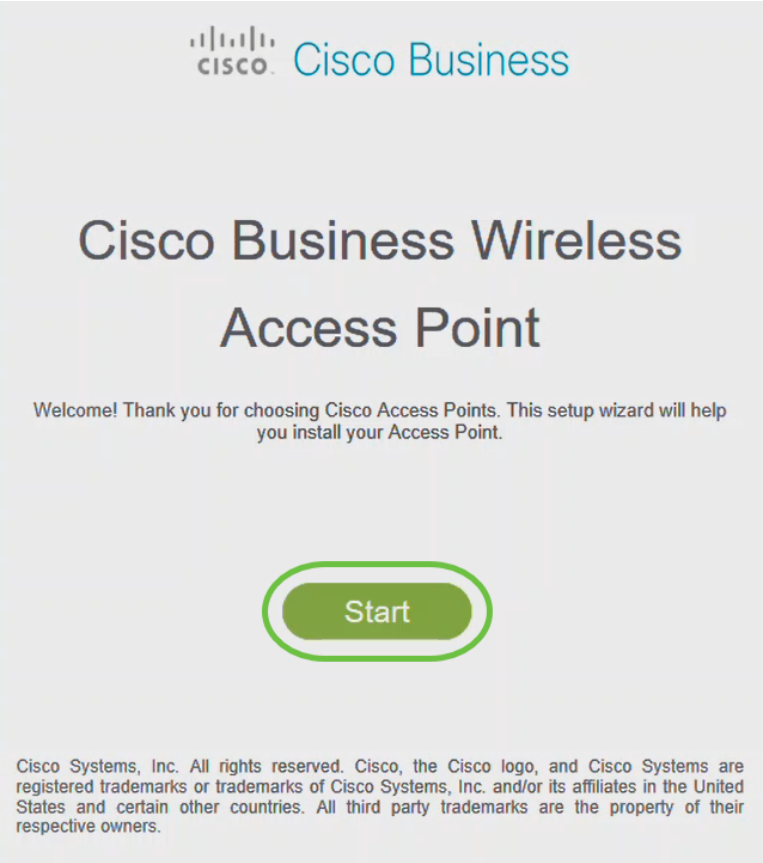
Você receberá a seguinte tela. Como você pode configurar apenas um dispositivo por vez, clique em **Não**.



Apenas um dispositivo pode ser conectado ao SSID *Cisco Business-Setup*. Se um segundo dispositivo tentar se conectar, ele não poderá. Se você não puder se conectar ao SSID e tiver validado a senha, talvez outro dispositivo tenha feito a conexão. Reinicie o AP e tente novamente.

Passo 4

Depois de conectado, o navegador da Web deve redirecionar automaticamente para o assistente de configuração do AP CBW. Caso contrário, abra um navegador da Web, como Internet Explorer, Firefox, Chrome ou Safari. Na barra de endereços, digite **http://ciscobusiness.cisco** e pressione **Enter**. Clique em **Iniciar** na página da Web.



Se você não vir a página da Web, aguarde mais alguns minutos ou recarregue a página. Após essa configuração inicial, você usará https://ciscobusiness.cisco para fazer login. Se o seu navegador da Web for preenchido automaticamente com *http://*, você precisará digitar manualmente *https://* para obter acesso.

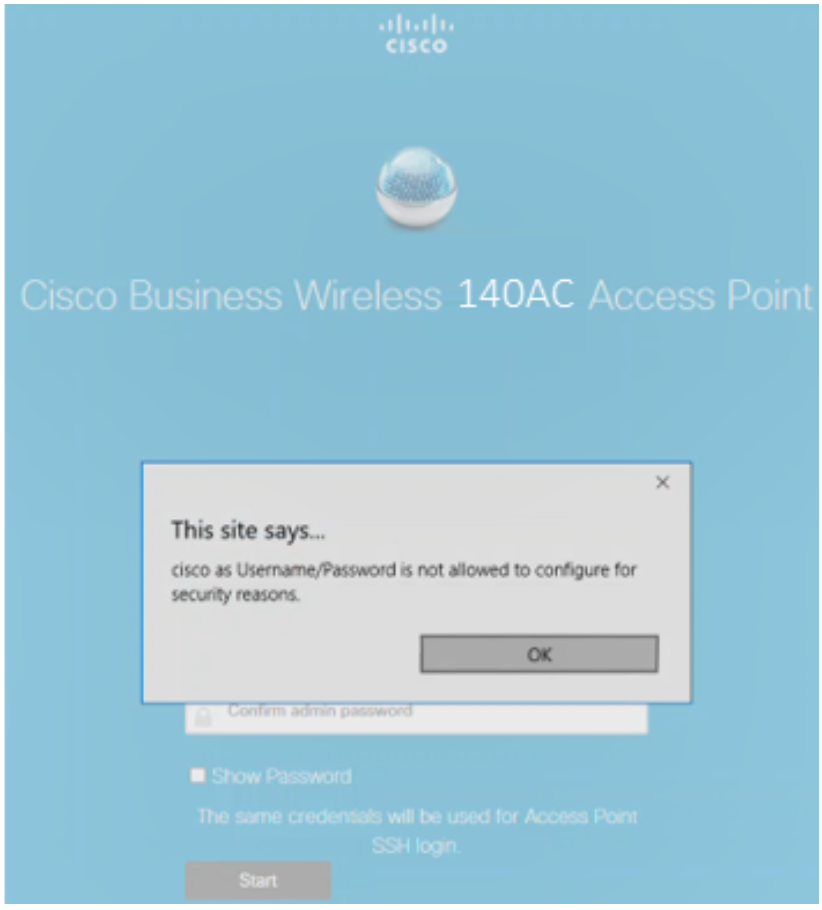
Etapa 5

Crie uma *conta admin* inserindo o seguinte:

- Nome de usuário do administrador (máximo de 24 caracteres)
- Senha do administrador
- Confirmar senha do administrador

Você pode escolher mostrar a senha marcando a caixa de seleção ao lado de *Mostrar senha*. Clique em Iniciar.

Não use *cisco* ou suas variações nos campos nome de usuário ou senha. Em caso afirmativo, você receberá uma mensagem de erro, conforme mostrado abaixo.

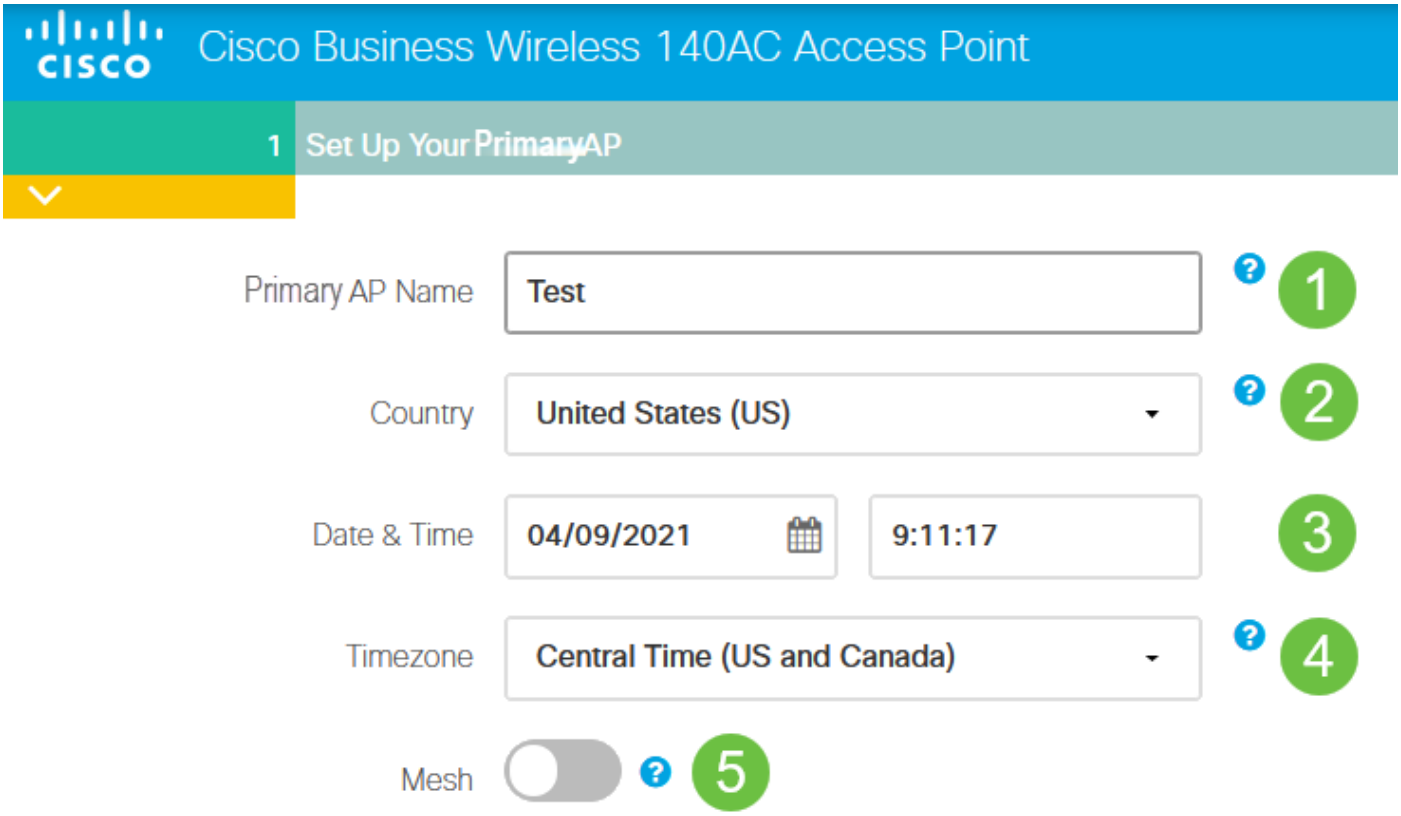


Etapa 6

Configure seu AP primário inserindo o seguinte:

- Nome do AP principal
- País

- Data e hora
- Fuso horário
- Malha



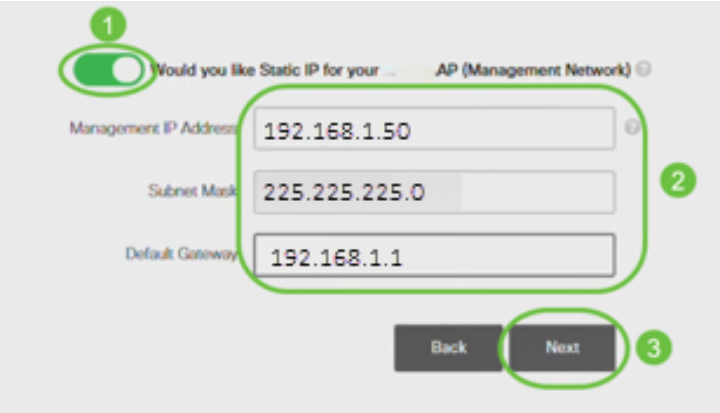
A malha deve ser habilitada somente se você planeja criar uma rede em malha. Por padrão, ele é desativado.

Etapa 7

(Opcional) Você pode habilitar o *IP estático para seu* CBW140AC para fins de gerenciamento. Caso contrário, a interface obtém um endereço IP do servidor DHCP. Para configurar o IP estático, insira o seguinte:

- Endereço IP de gerenciamento
- Máscara de sub-rede
- Gateway padrão

Clique em Next.



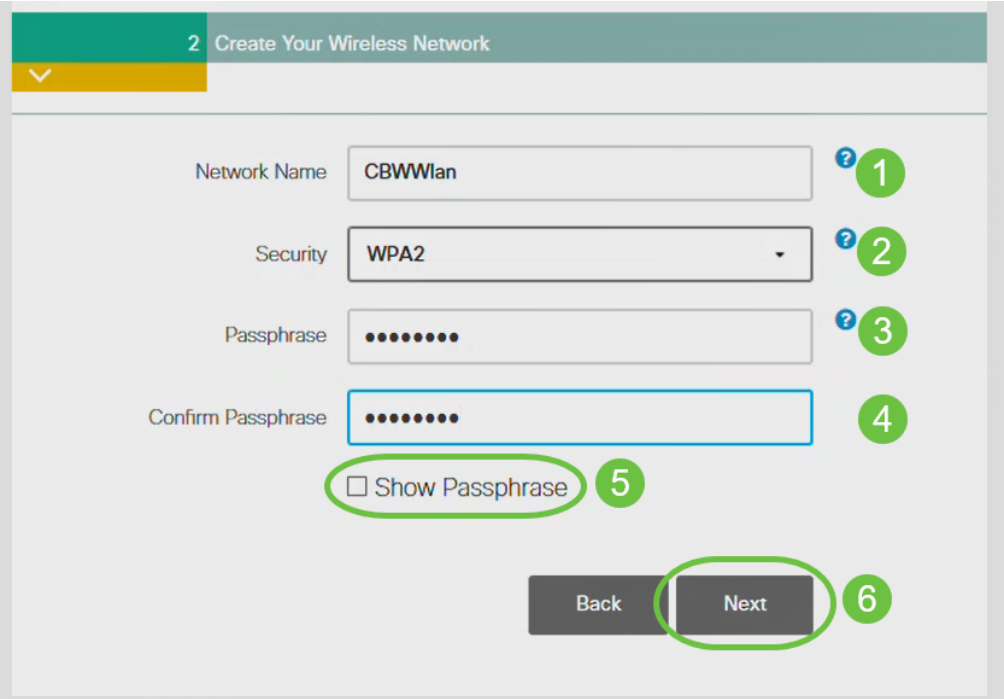
Por padrão, essa opção está desativada.

Passo 8

Crie suas redes sem fio inserindo o seguinte:

- Nome da rede
- Escolher segurança
- Senha
- Confirmar senha
- (Opcional) Marque a caixa de seleção para Mostrar senha.

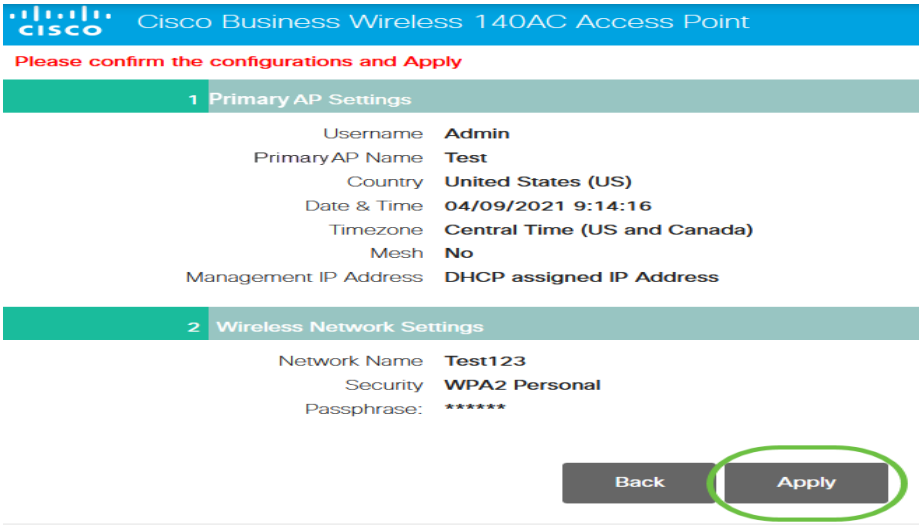
Clique em Next.



O WPA (Wi-Fi Protected Access) versão 2 (WPA2) é o padrão atual para segurança Wi-Fi.

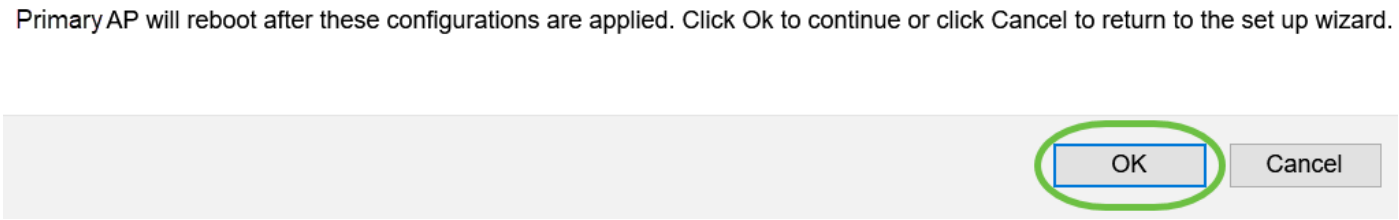
Passo 9

Confirme as configurações e clique em **Aplicar**.

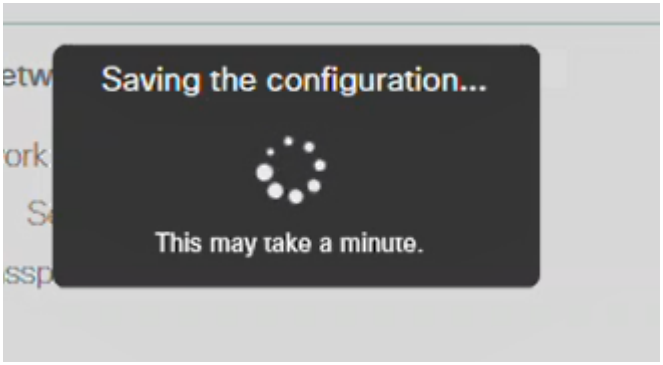


Passo 10

Clique em **OK** para aplicar as configurações.



Você verá a tela a seguir enquanto as configurações estiverem sendo salvas e o sistema for reinicializado. Isso pode levar 10 minutos.

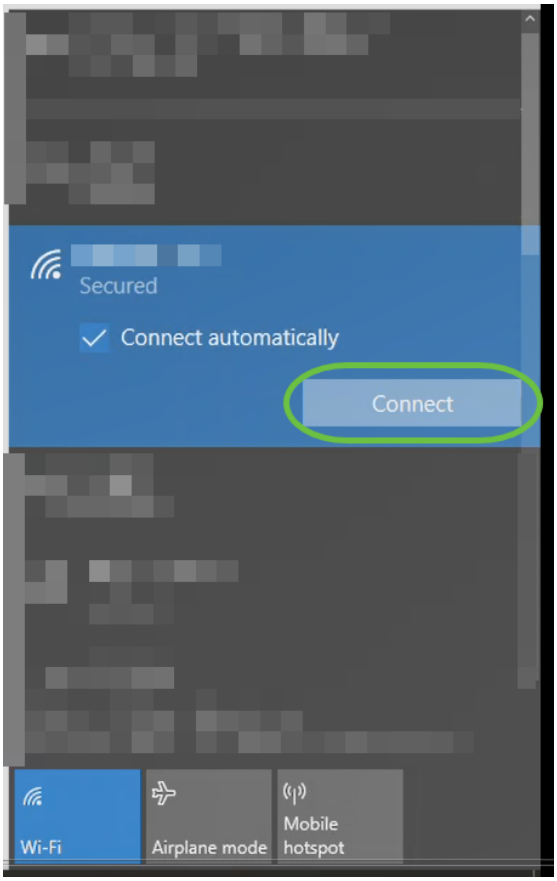


Durante a reinicialização, o LED no ponto de acesso passará por vários padrões de cores. Quando o LED estiver piscando em verde, vá para a próxima etapa. Se o LED não ultrapassar o padrão vermelho piscante, isso indica que não há servidor DHCP em sua rede. Verifique se o AP está conectado a um switch ou roteador com um servidor DHCP.

Passo 11

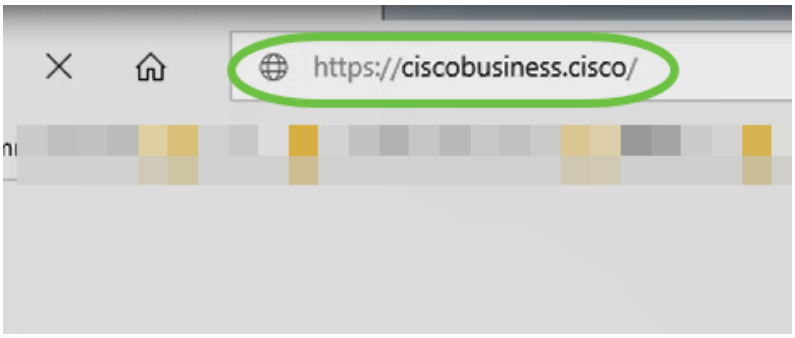
Vá para as opções sem fio do PC e escolha a rede que você configurou. Clique em Conectar.

O SSID *Cisco Business-Setup* desaparecerá após a reinicialização.



Etapa 12

Abra um navegador da Web e digite *https://[endereço IP do AP CBW]*. Como alternativa, você pode digitar *https://ciscobusiness.cisco* na barra de endereços e pressionar Enter.



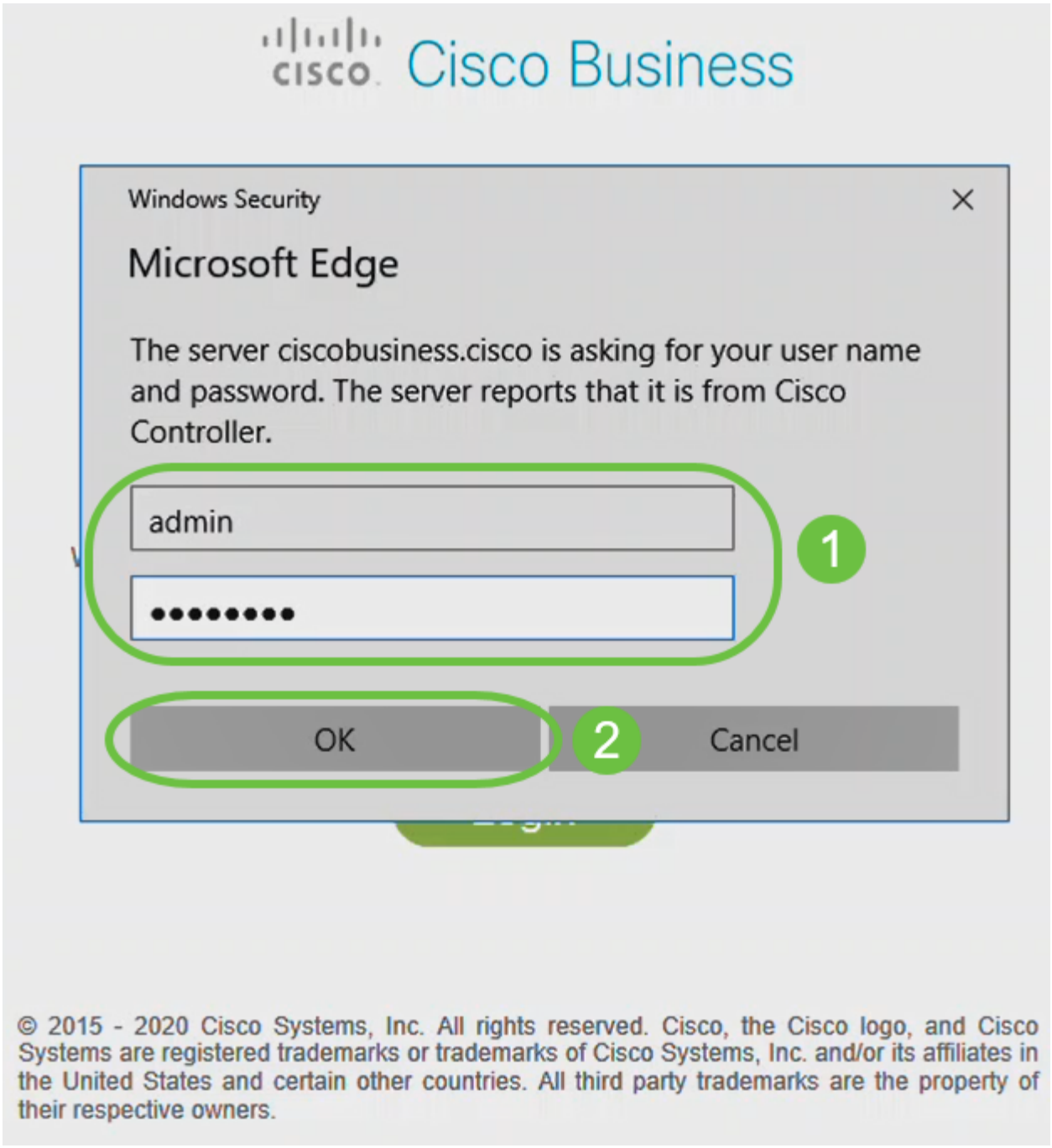
Certifique-se de digitar *https* e não *http* nesta etapa.

Passo 13

Clique em login.

Passo 14

Faça login usando as credenciais configuradas. Click OK.



Etapa 15

Você poderá acessar a página da IU da Web do AP.

Dicas para solução de problemas sem fio

Se tiver problemas, dê uma olhada nas seguintes dicas:

- Verifique se o SSID (Service Set Identifier, Identificador do conjunto de serviços) correto está selecionado. Este é o nome que você criou para a rede sem fio.
- Desconecte qualquer VPN do aplicativo móvel ou de um laptop. Você pode até estar conectado a uma VPN que o seu provedor de serviços móveis usa e que você talvez nem saiba. Por exemplo, um telefone Android (Pixel 3) com Google Fi como provedor de serviços, há uma VPN integrada que se conecta automaticamente sem notificação. Isso precisaria ser desabilitado para encontrar o AP primário.
- Efetue login no AP primário com https://<endereço IP do AP primário>.
- Depois de fazer a configuração inicial, certifique-se de que https:// is esteja sendo usado para fazer login no *ciscobusiness.cisco* ou inserindo o endereço IP no navegador da Web. Dependendo das suas configurações, o computador pode ter sido preenchido automaticamente com http:// since, que é o que você usou na primeira vez em que se conectou.
- Para ajudar com problemas relacionados ao acesso à interface do usuário da Web ou problemas do navegador durante o uso do AP, no navegador da Web (neste caso, Firefox), clique no menu Abrir, vá para Ajuda > Informações de solução de problemas e clique em Atualizar Firefox.

Configure os extensores de malha CBW142ACM usando a interface de usuário da Web

Você está na parte inicial da configuração dessa rede, basta adicionar seus extensores de malha!

Passo 1

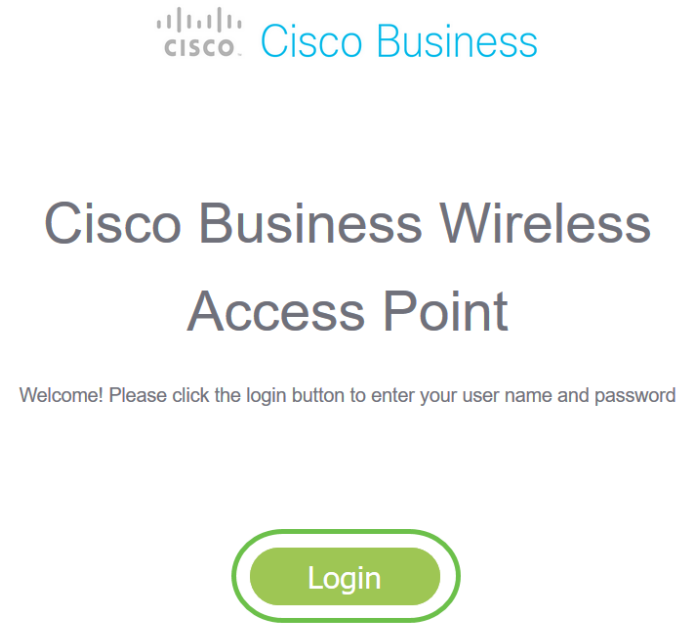
Conecte os dois extensores de malha na parede nos locais selecionados. Anote o endereço MAC de cada extensor de malha.

Passo 2

Aguarde cerca de 10 minutos até que o Mesh Extenders seja inicializado.

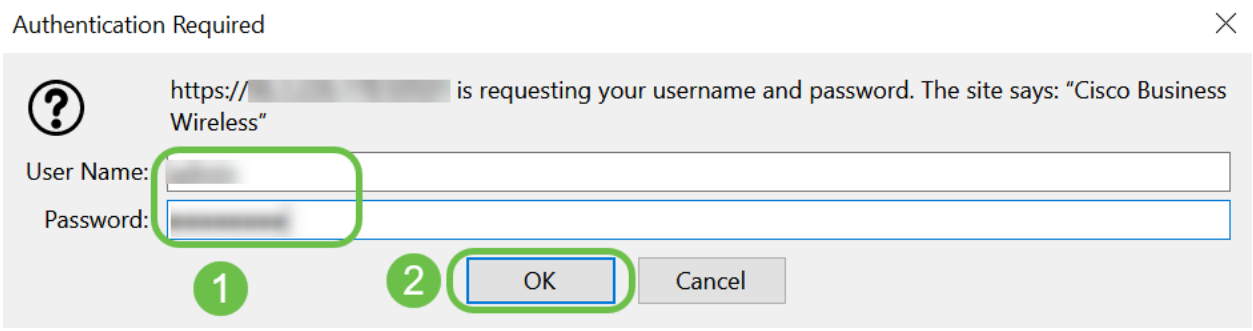
Etapa 3

Insira o endereço IP dos pontos de acesso primários (APs) no navegador da Web. Clique em **Login** para acessar o AP primário.



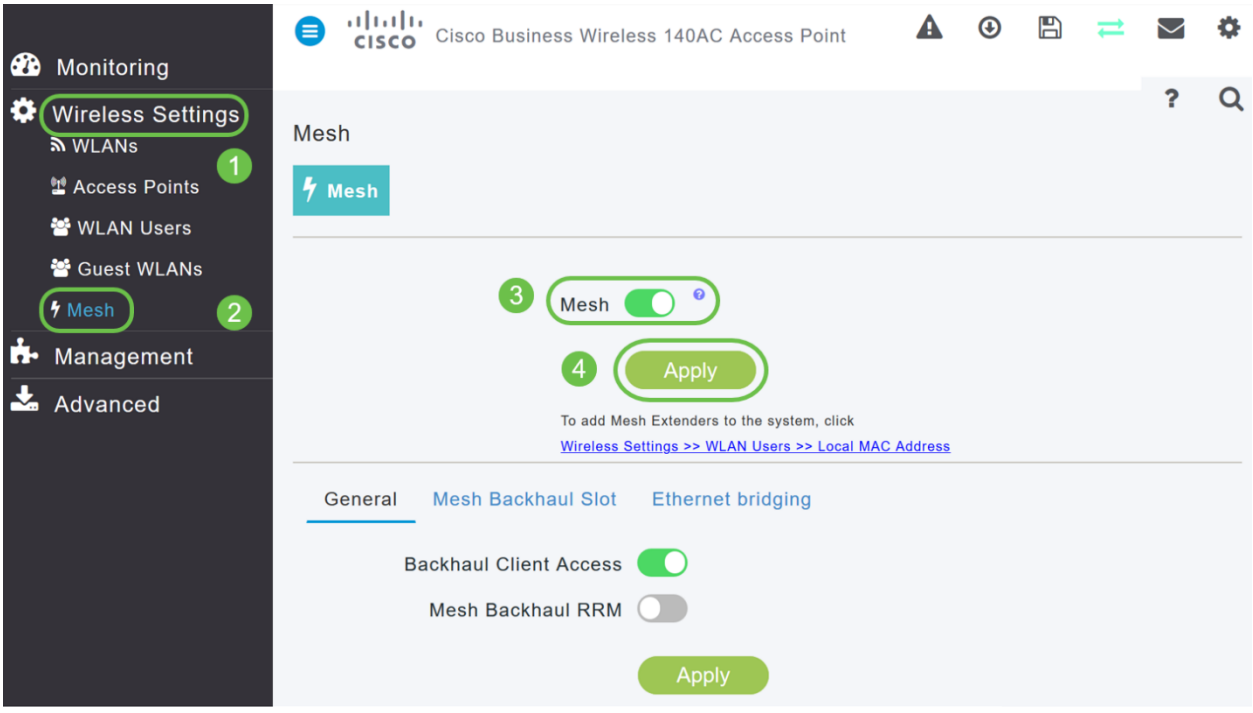
Passo 4

Insira suas credenciais *de Nome de usuário* e *Senha* para acessar o AP primário. Click OK.



Etapa 5

Navegue até **Wireless Settings > Mesh**. Verifique se a *malha* está ativada. Clique em Apply.

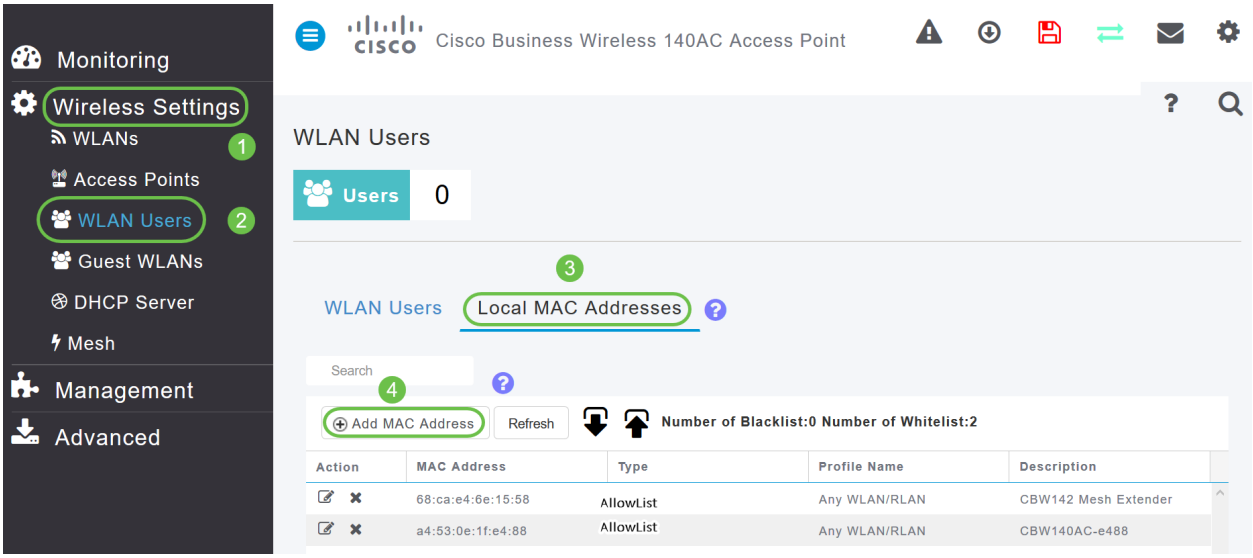


Etapa 6

Se Mesh ainda não estiver habilitada, o WAP pode precisar executar uma reinicialização. Uma janela pop-up será exibida para fazer uma reinicialização. Confirme. Isso levará cerca de 10 minutos. Durante uma reinicialização, o LED piscará em verde em vários padrões, alternando rapidamente entre verde, vermelho e âmbar antes de ficar verde novamente. Pode haver pequenas variações na intensidade da cor do LED e na tonalidade de unidade para unidade.

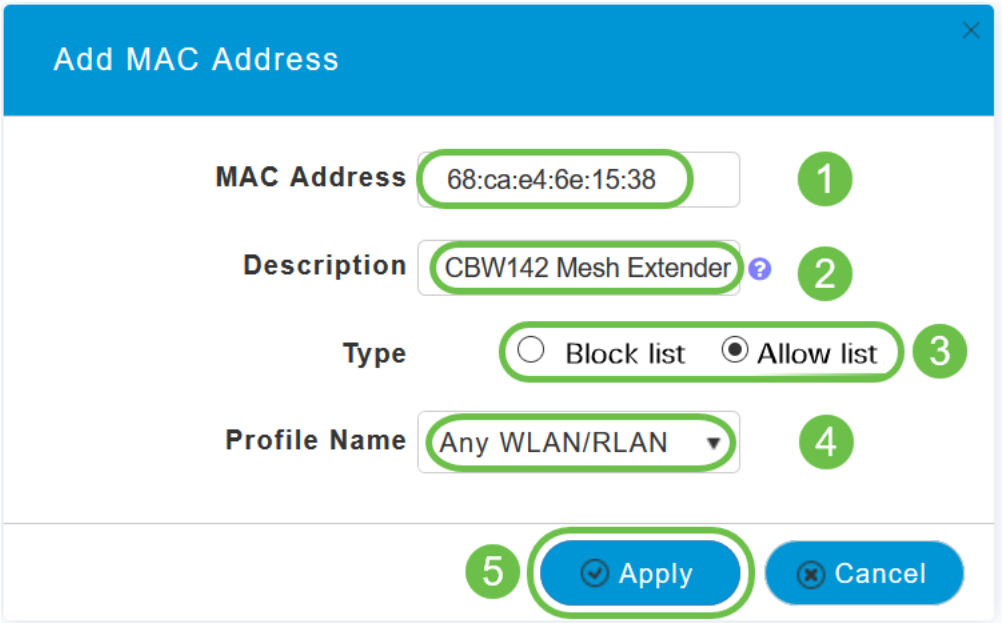
Etapa 7

Navegue até **Wireless Settings > WLAN Users > Local MAC Addresses**. Clique em **Adicionar endereço MAC**.



Passo 8

Insira o endereço MAC e a descrição do extensor de malha. Selecione a lista *Tipo* como Permitir. Selecione o *nome do perfil* no menu suspenso. Clique em Apply.



Passo 9

Certifique-se de salvar todas as configurações pressionando o **ícone salvar** no painel superior direito da tela.

Repita para cada extensor de malha.

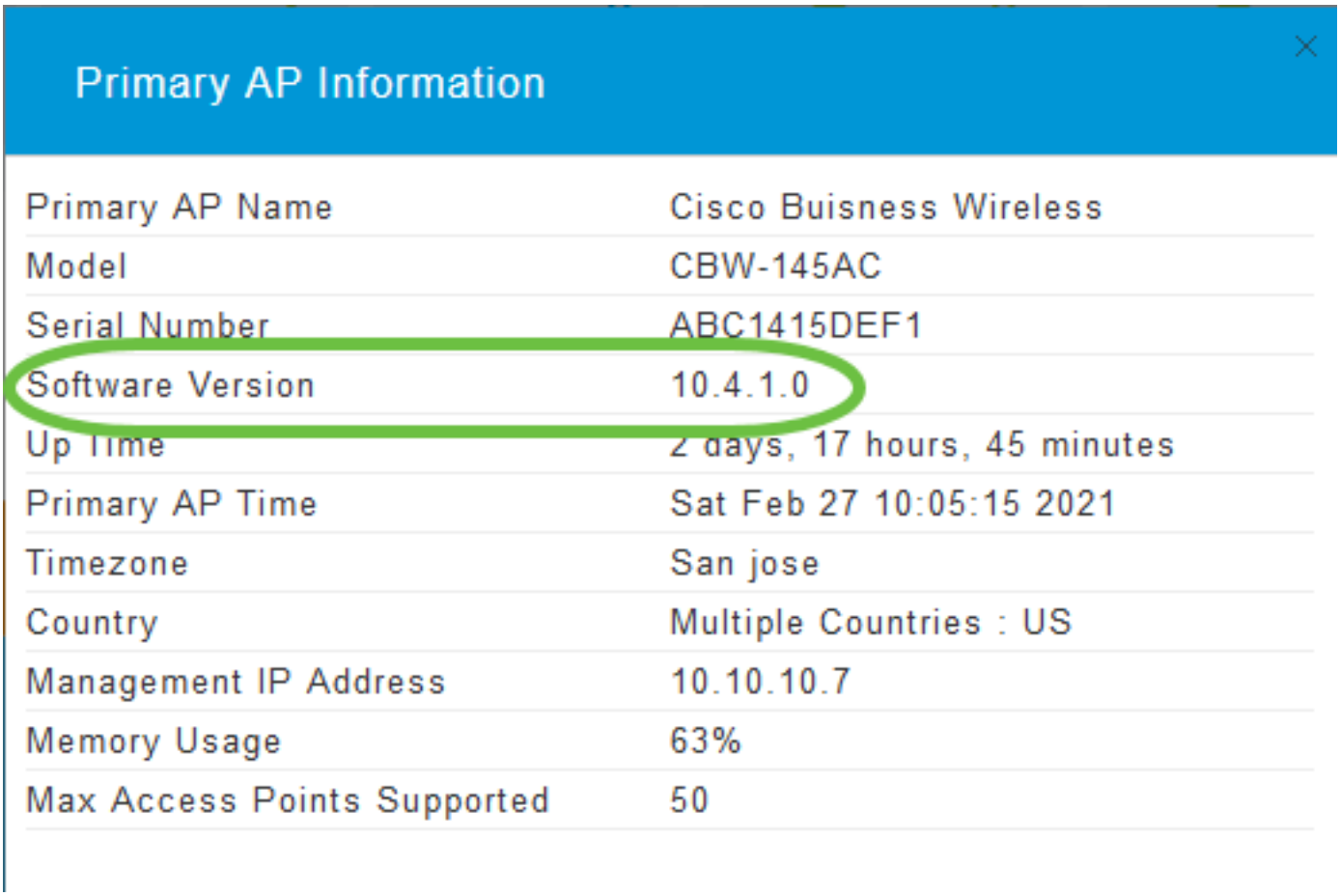
Verificar e atualizar o software usando a interface de usuário da Web

Não ignore esta etapa importante! Há algumas maneiras de atualizar o software, mas as etapas listadas abaixo são recomendadas como as mais fáceis de executar quando você usa a IU da Web.

Para exibir e atualizar a versão atual do software do seu AP primário, execute as seguintes etapas.

Passo 1

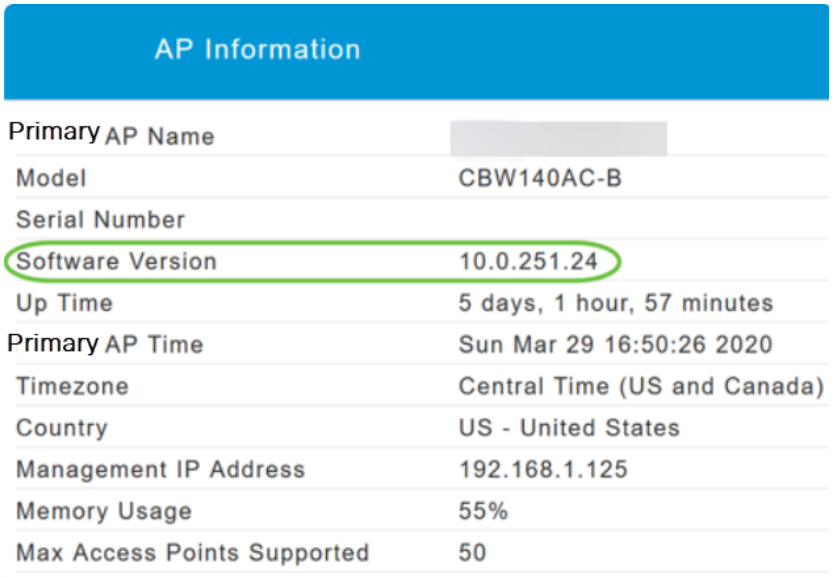
Clique no **ícone da engrenagem** no canto superior direito da interface da Web e clique em **Primary AP Information (Informações principais do AP)**.



Passo 2

Compare a versão que está sendo executada com a versão de software mais recente.

Feche a janela quando souber se precisa atualizar o software.

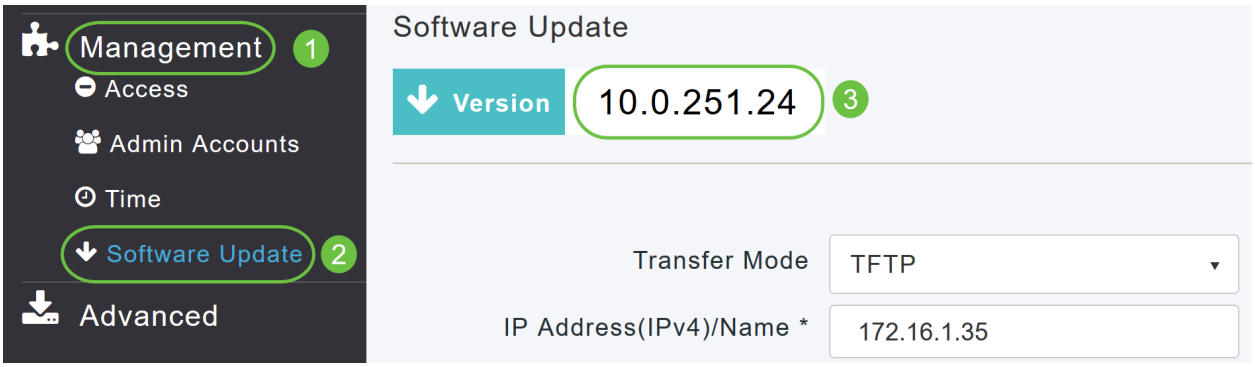


Se estiver executando a versão mais recente do software, você poderá ir para a seção Criar WLANs.

Etapa 3

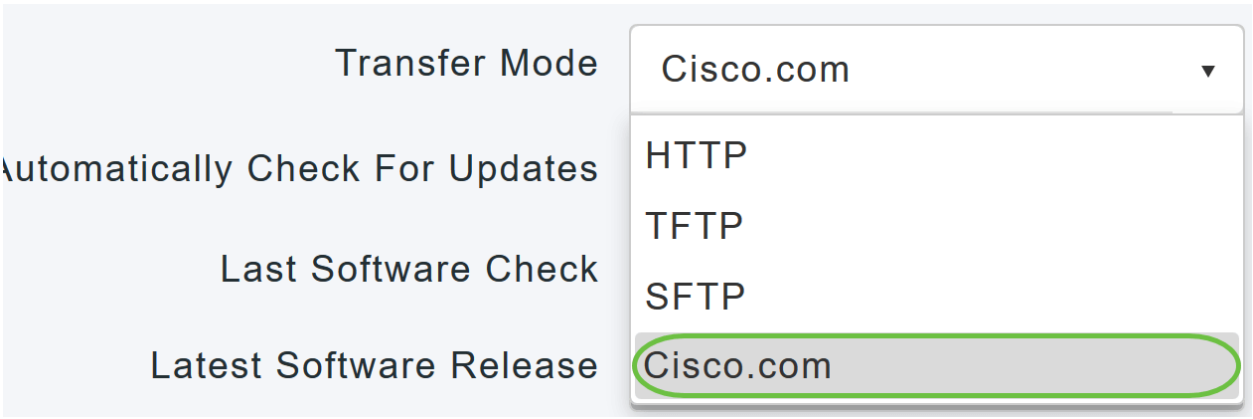
Escolha **Management > Software Update** no menu.

A janela *Software Update* é exibida com o número de versão do software atual listado na parte superior.



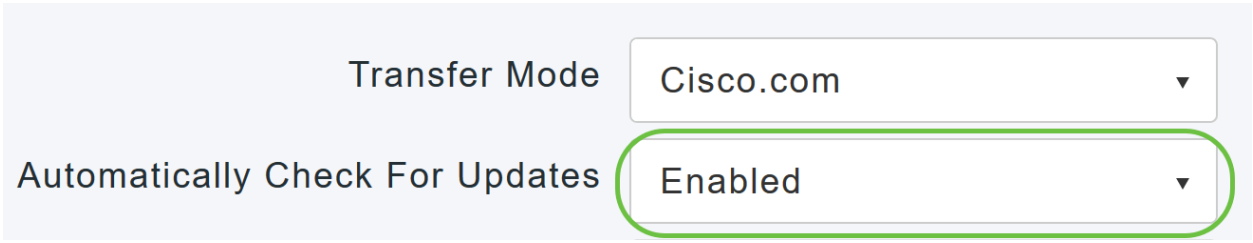
Você pode atualizar o software de AP CBW e as configurações atuais no AP primário não serão excluídas.

Na lista suspensa *Modo de transferência*, escolha **Cisco.com**.



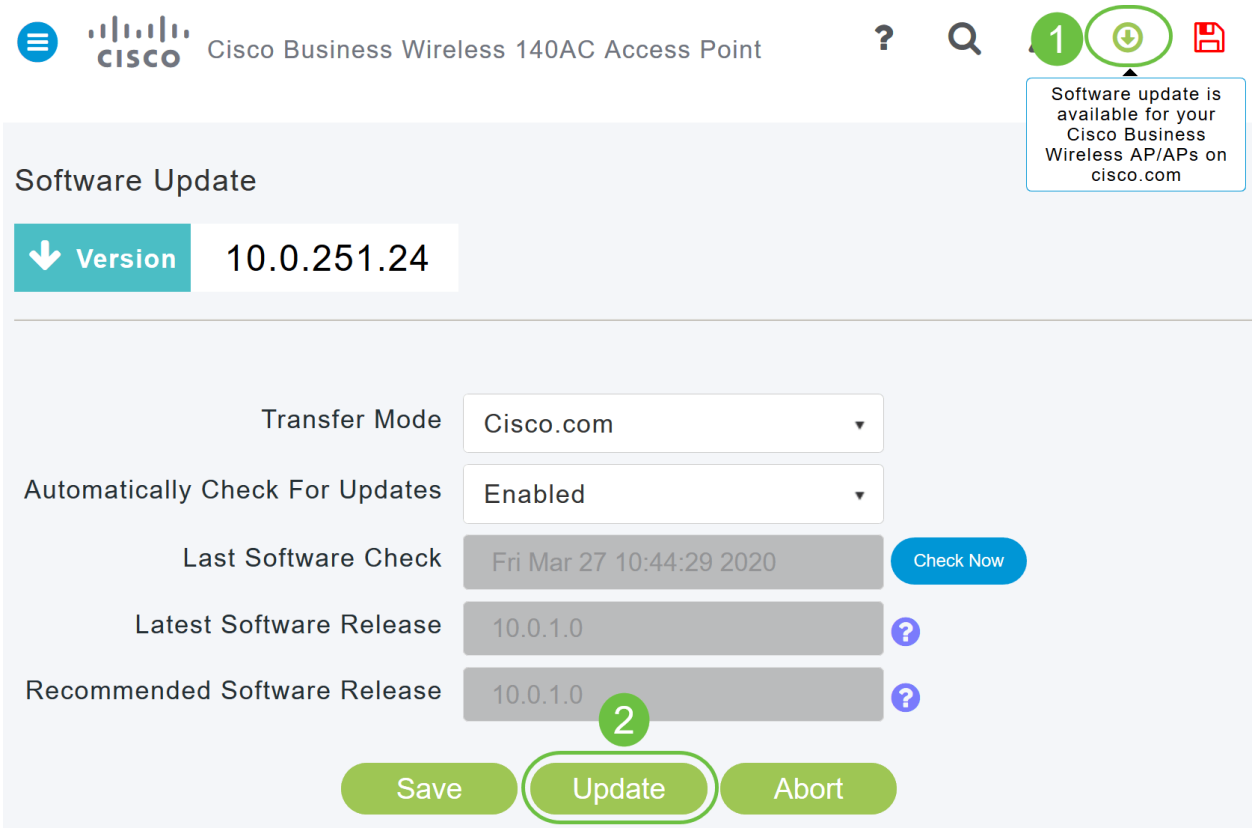
Passo 4

Para definir o AP primário para verificar automaticamente as atualizações de software, escolha **Enabled (Habilitado)** na lista suspensa *Automatically Check for Updates (Verificar automaticamente as atualizações)*. Iss está habilitado por padrão.



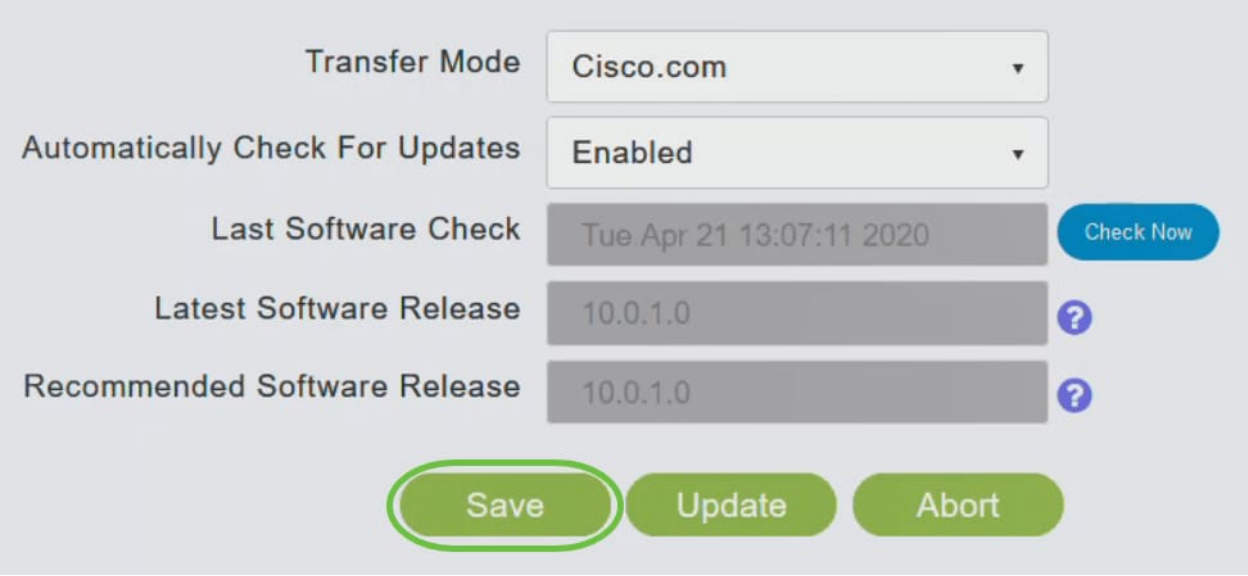
Quando uma verificação de software é feita e se uma atualização de software mais recente ou recomendada está disponível no Cisco.com, então:

- O **ícone de alerta de atualização de software** no canto superior direito da IU da Web estará verde (ou cinza). Clicar no ícone o levará à página Atualização de software.
- O botão Update (Atualizar) na parte inferior da página *Software Update (Atualização de software)* está ativado.

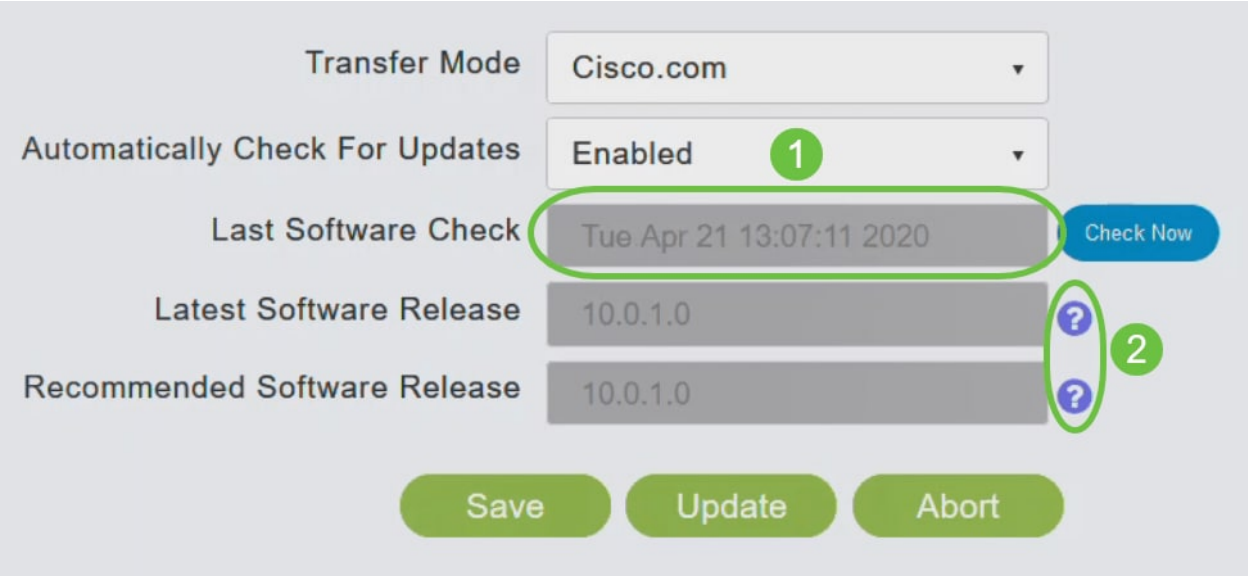


Etapa 5

Click Save. Isso salva as entradas ou alterações feitas em ambos os *modos de transferência* e *verifica automaticamente se há atualizações*.

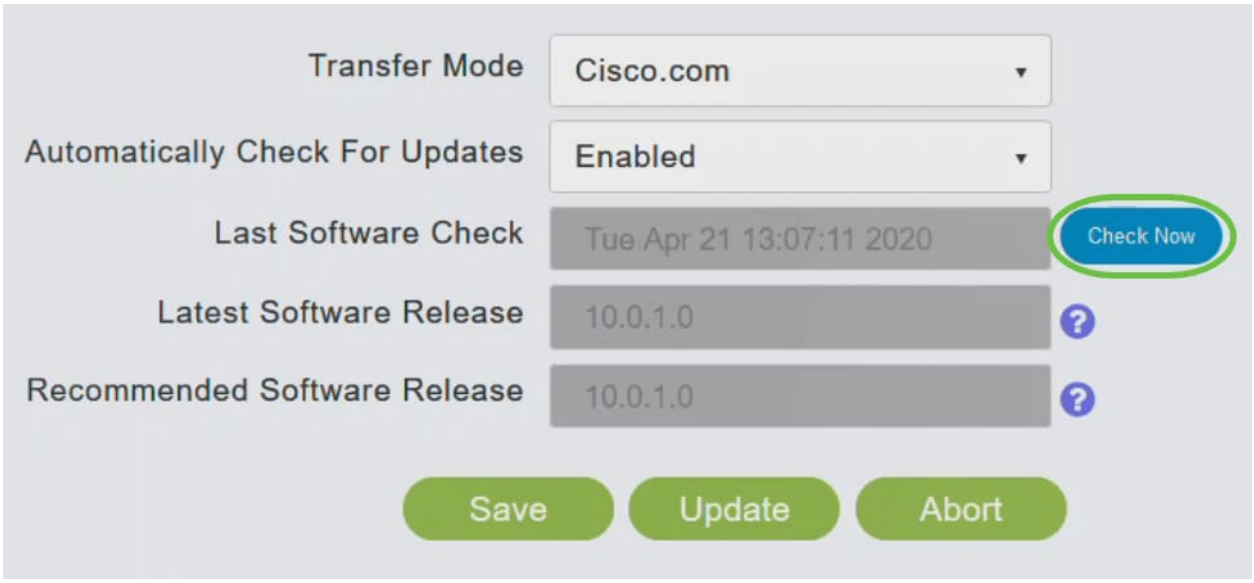


O campo *Última verificação de software* exibe o carimbo de data e hora da última verificação automática ou manual de software. Você pode ver as notas das versões exibidas clicando no **ícone de ponto de interrogação** ao lado.



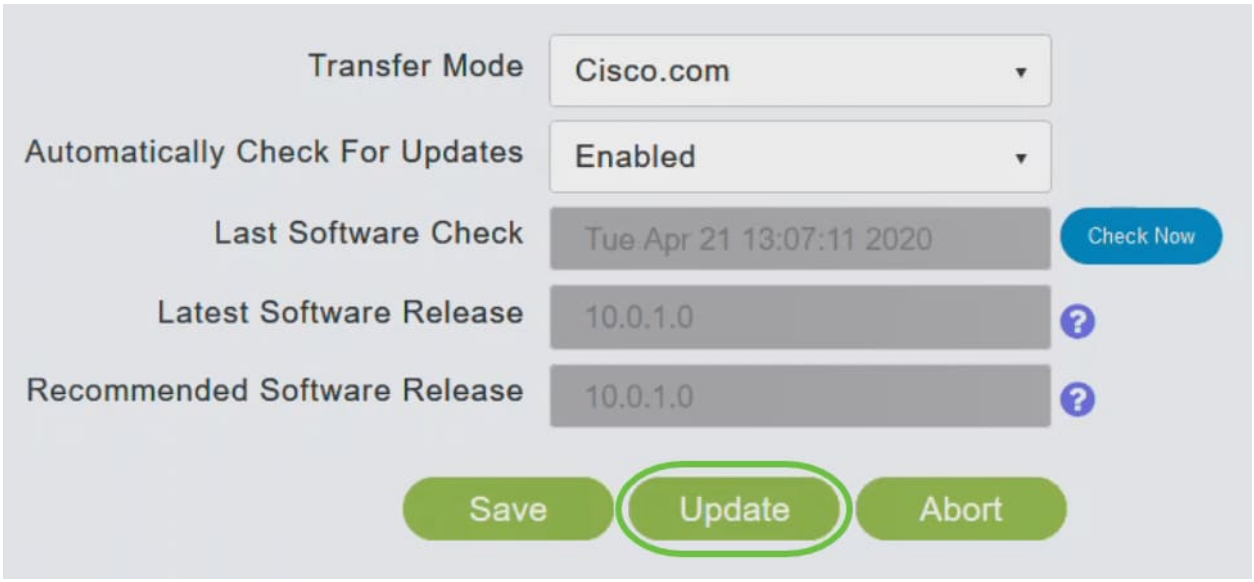
Etapa 6

Você pode executar manualmente uma verificação de software a qualquer momento clicando em *Verificar agora*.



Etapa 7

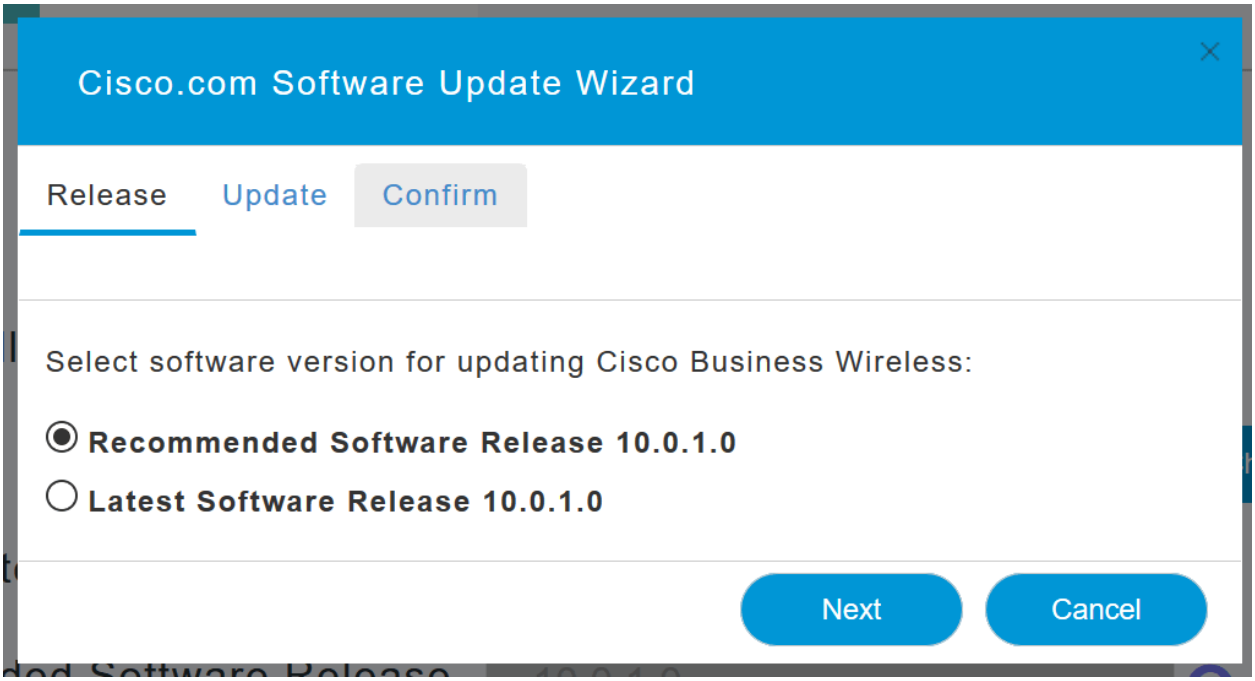
Para continuar com a atualização do software, clique em **Atualizar**.



O *Assistente de atualização de software* é exibido. O assistente exibe as três guias a seguir em sequência:

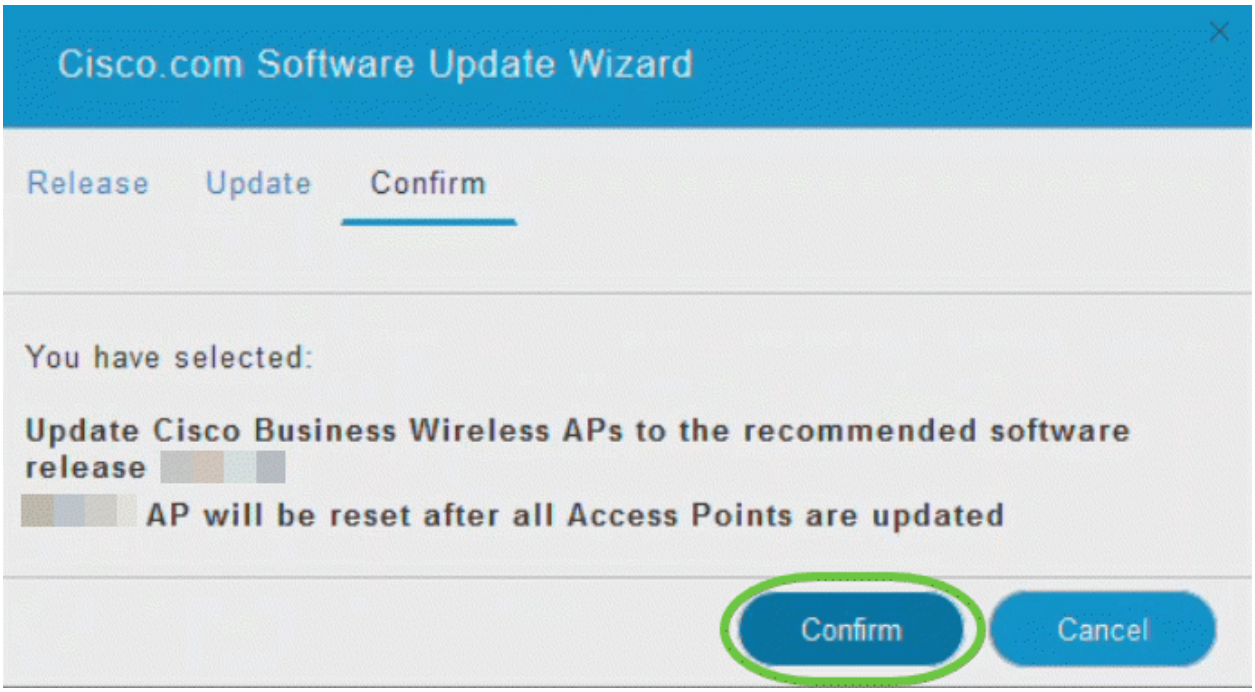
- Guia Versão - Especifique se deseja atualizar para a versão de software recomendada ou para a versão de software mais recente.
- Guia Atualizar - Especifique quando os APs devem ser redefinidos. Você pode optar por fazê-lo imediatamente ou agendá-lo para um horário posterior. Para configurar o AP primário para reinicializar automaticamente após a conclusão do pré-download da imagem, marque a caixa de seleção Reiniciar automaticamente.
- Confirmar guia - Confirme suas seleções.

Siga as instruções do assistente. Você pode voltar para qualquer guia a qualquer momento antes de clicar em *Confirmar*.



Passo 8

Clique em **Confirmar**.

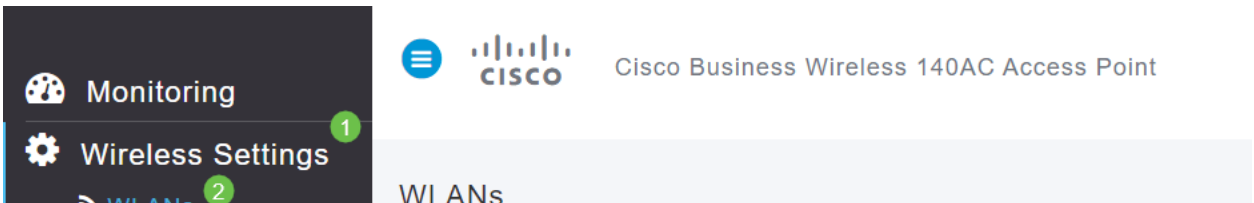


Criar WLANs na IU da Web

Esta seção permite criar redes locais sem fio (WLANs).

Passo 1

Uma WLAN pode ser criada navegando para **Wireless Settings > WLANs**. Em seguida, selecione **Add new WLAN/RLAN**.



Passo 2

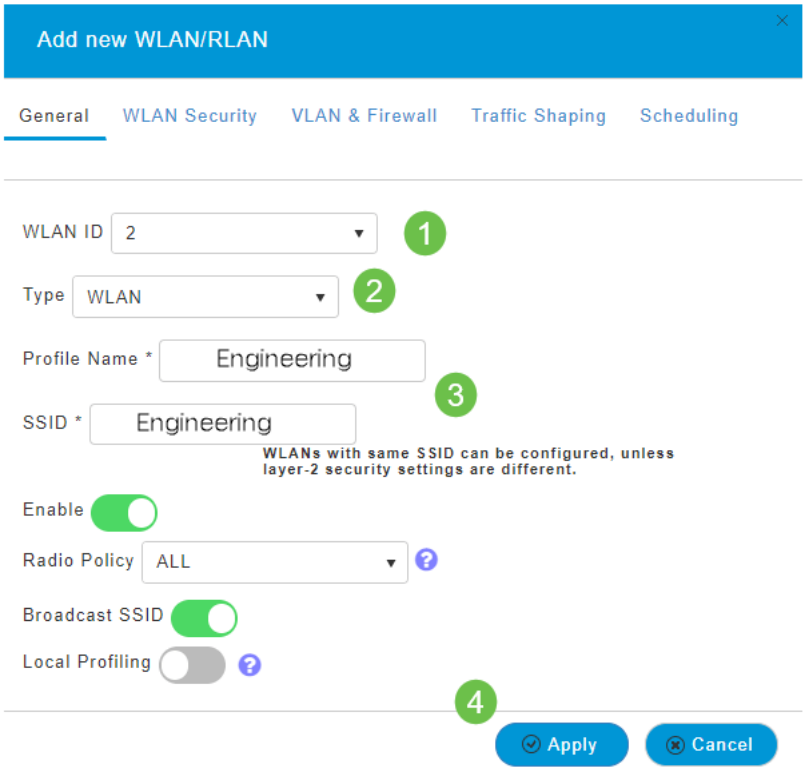
Na guia *Geral*, insira as seguintes informações:

- ID da WLAN - Selecione um número para a WLAN
- Tipo - Selecionar **WLAN**
- Nome do perfil - Ao inserir um nome, o SSID será preenchido automaticamente com o mesmo nome. O nome deve ser exclusivo e não deve exceder 31 caracteres.

Os campos a seguir foram deixados como padrão neste exemplo, mas as explicações são listadas caso você queira configurá-los de forma diferente.

- SSID - O nome do perfil também atua como SSID. Você pode alterar isso se desejar. O nome deve ser exclusivo e não deve exceder 31 caracteres.
- Habilitar - Deve ser deixado habilitado para que a WLAN funcione.
- Política de rádio - Normalmente, você gostaria de deixar isso como **tudo** para que os clientes de 2,4 GHz e 5 GHz possam acessar a rede.
- SSID de transmissão - normalmente, você deseja que o SSID seja descoberto, portanto, deixe-o como Ativado.
- Criação de perfil local - Deseja habilitar essa opção apenas para exibir o sistema operacional que está sendo executado no cliente ou para ver o nome do usuário.

Clique em Apply.



Etapa 3

Você será direcionado para a guia *WLAN Security*.

Neste exemplo, as seguintes opções foram deixadas como padrão:

- A rede do convidado, o Captive Network Assistant e a filtragem de MAC foram deixados desabilitados. Os detalhes da configuração de uma rede de convidado estão detalhados na próxima seção.
- WPA2 Personal - Wi-Fi Protected Access 2 com PSK (Pre-shared Key, Formato de senha de chave pré-compartilhada) - ASCII. Esta opção significa Wi-Fi Protected Access 2 com chave pré-compartilhada (PSK).

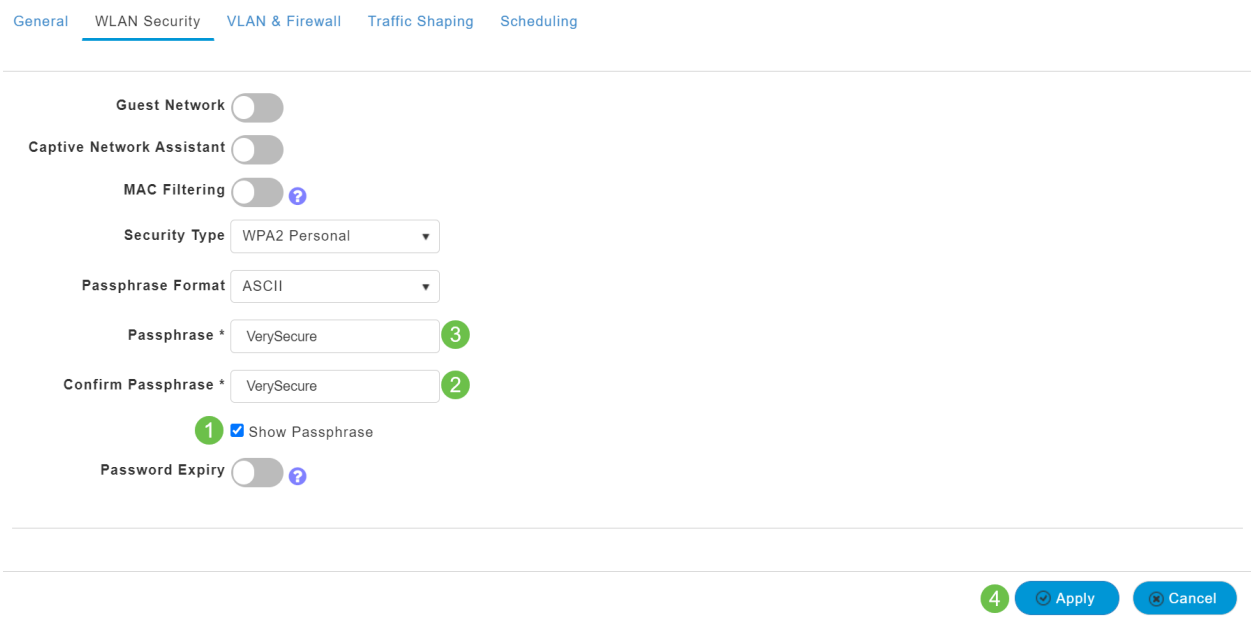
WPA2 Personal é um método usado para proteger sua rede com o uso de uma autenticação PSK. A PSK é configurada separadamente no AP primário, na política de segurança da WLAN e no cliente. A WPA2 Personal não depende de um servidor de autenticação na sua rede.

- Formato de Senha - **ASCII é deixado como padrão.**

Os seguintes campos foram inseridos neste cenário:

- Show Passphrase - (Mostrar senha) clique na caixa de seleção para ver a senha inserida.
- Passphrase - (Senha) Insira um nome para a senha (senha).
- Confirmar senha - Insira a senha novamente para confirmá-la.

Clique em Apply. Isso ativará automaticamente a nova WLAN.

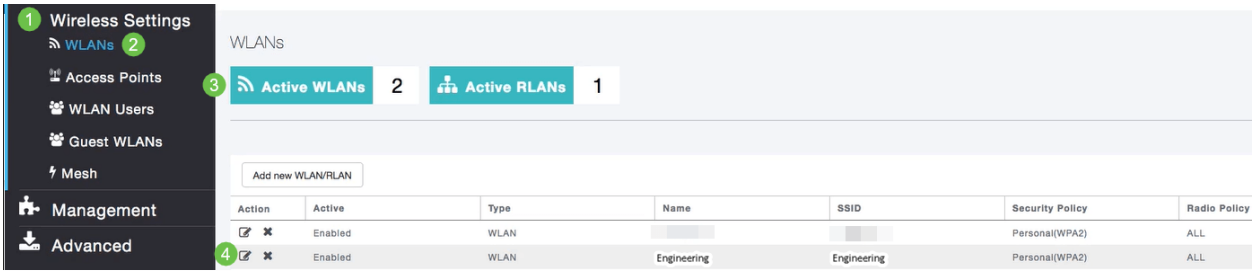


Passo 4

Certifique-se de salvar suas configurações clicando no **ícone salvar** no painel superior direito da tela da IU da Web.

Etapa 5

Para ver a WLAN que você criou, selecione **Wireless Settings > WLANs**. Você verá o número de WLANs ativas elevado a 2 e a nova WLAN será exibida.



Repita essas etapas para outras WLANs que você deseja criar.

Configurações sem fio opcionais

Agora você tem todas as configurações básicas definidas e estão prontas para serem implementadas. Você tem algumas opções, então sinta-se à vontade para ir para qualquer uma das seguintes seções:

- Crie uma WLAN de Convidado usando a IU da Web (Opcional)
- Criação de perfis de aplicativos (opcional)
- Criação de perfis de clientes (opcional)
- Estou pronto para concluir isso e começar a usar minha rede!

Crie uma WLAN de Convidado usando a IU da Web (Opcional)

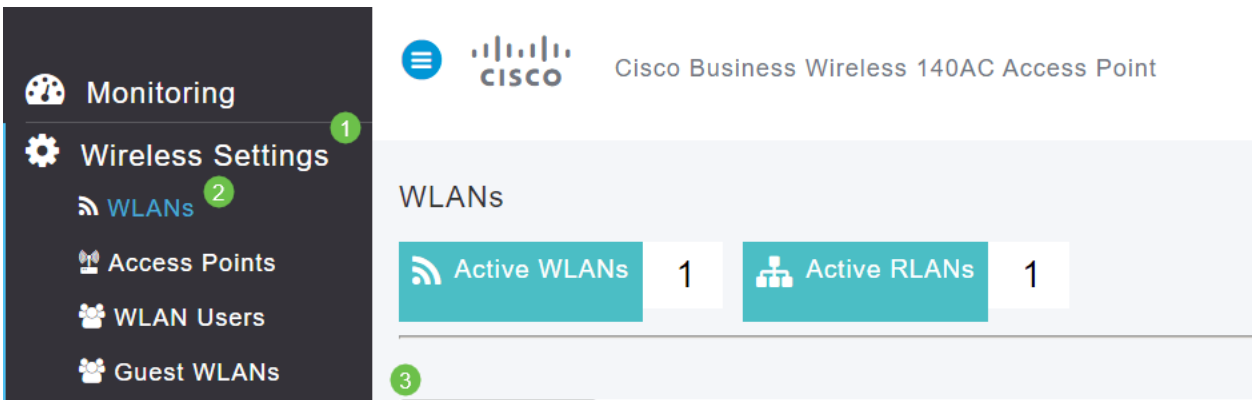
Uma WLAN de convidado fornece acesso de convidado à sua rede Cisco Business Wireless.

Passo 1

Efetue login na IU da Web do AP primário. Abra um navegador da Web e digite www.https://ciscobusiness.cisco. Você pode receber um aviso antes de continuar. Digite suas credenciais. Você também pode acessá-lo inserindo o endereço IP do AP primário.

Passo 2

Uma rede local sem fio (WLAN) pode ser criada navegando para **Wireless Settings > WLANs**. Em seguida, selecione **Add new WLAN/RLAN**.



Etapa 3

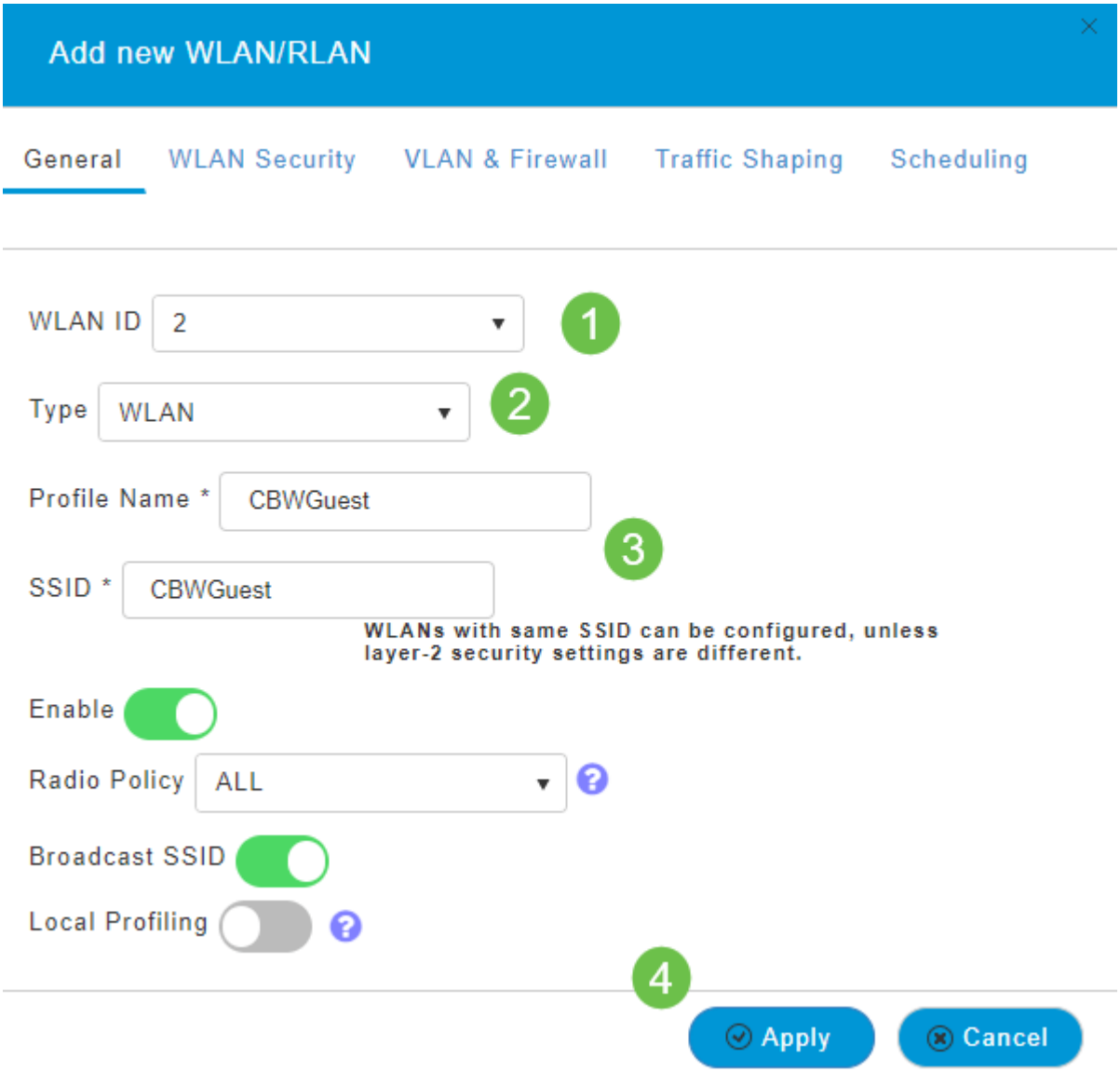
Na guia *Geral*, insira as seguintes informações:

WLAN ID - Selecione um número para a WLAN
Tipo - Selecionar **WLAN**
Nome do perfil - Quando você digita um nome, o SSID será preenchido automaticamente com o mesmo nome. O nome deve ser exclusivo e não deve exceder 31 caracteres.

Os campos a seguir foram deixados como padrão neste exemplo, mas as explicações são listadas caso você queira configurá-los de forma diferente.

SSID - O nome do perfil também atua como SSID. Você pode alterar isso se desejar. O nome deve ser exclusivo e não deve exceder 31 caracteres.
Habilitar - Deve ser deixado habilitado para que a WLAN funcione.
Política de rádio - Normalmente, você gostaria de deixar isso como **tudo** para que os clientes de 2,4 GHz e 5 GHz possam acessar a rede.
SSID de transmissão - Normalmente, você deseja que o SSID seja descoberto, portanto, deixe-o como Ativado.
Criação de perfil local - Só pretende ativar esta opção para ver o sistema operacional que está a ser executado no cliente ou para ver o nome de utilizador.

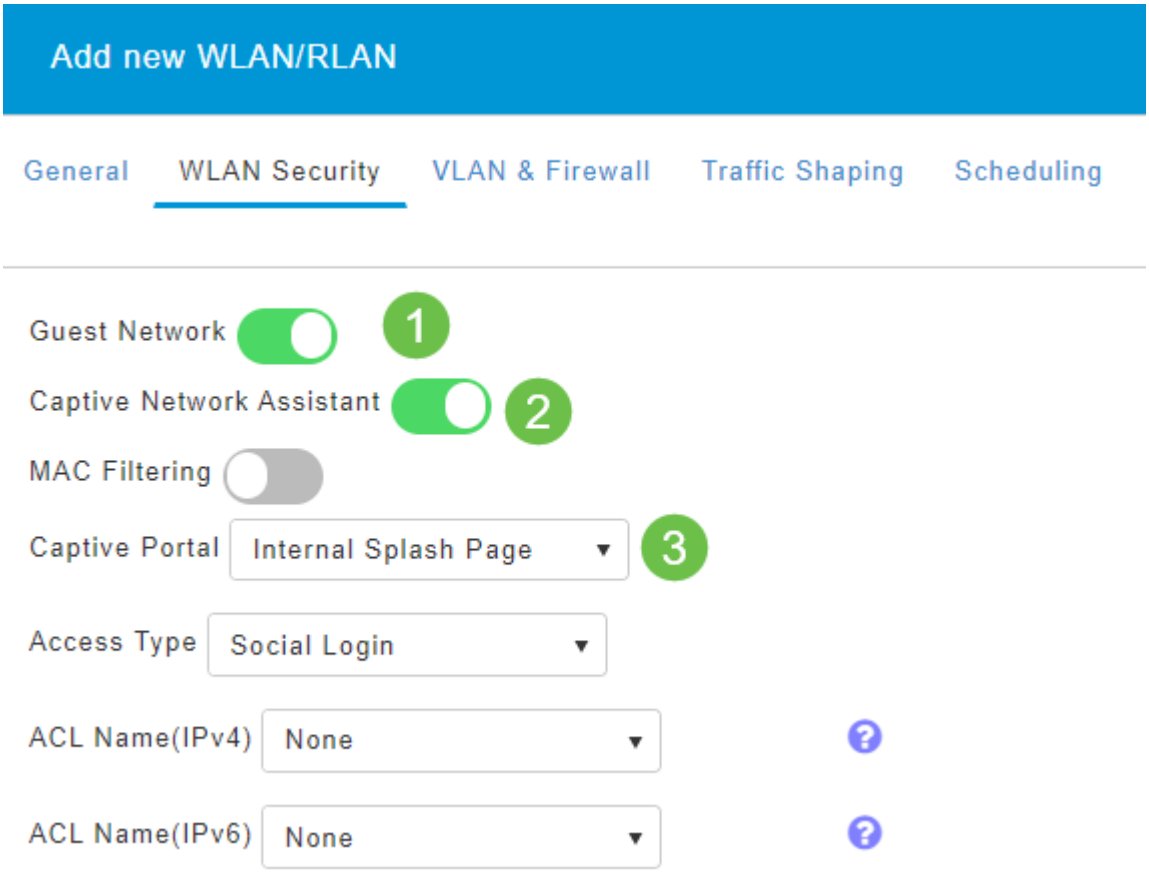
Clique em Apply.



Passo 4

Você será direcionado para a guia *WLAN Security*. Neste exemplo, as seguintes opções foram selecionadas.

- Rede de convidado - Habilitar
- Captive Network Assistant - Se você usa o Mac ou o IOS, provavelmente deseja habilitá-lo. Este recurso detecta a presença de um portal cativo enviando uma solicitação da Web ao conectar-se a uma rede sem fio. Esta solicitação é direcionada a um URL (Uniform Resource Locator) para modelos de iPhone e, se uma resposta for recebida, o acesso à Internet é considerado disponível e nenhuma outra interação é necessária. Se nenhuma resposta for recebida, o acesso à Internet será bloqueado pelo portal cativo e o Captive Network Assistant (CNA) da Apple iniciará automaticamente o pseudo-navegador para solicitar o login do portal em uma janela controlada. O CNA pode quebrar ao redirecionar para um portal cativo do Identity Services Engine (ISE). O AP primário impede que este pseudo-navegador apareça.
- Portal cativo - Esse campo fica visível somente quando a opção Rede de convidado está ativada. Isso é usado para especificar o tipo de portal da Web que pode ser usado para fins de autenticação. Selecione Página inicial interna para usar a autenticação padrão baseada no portal da Web da Cisco. Escolha External Splash Page se você tiver autenticação de portal cativo, usando um servidor Web fora da sua rede. Além disso, especifique a URL do servidor no campo URL do site.



Neste exemplo, a WLAN de convidado com um tipo de acesso de login social habilitado será criada. Quando o usuário se conectar a esta WLAN de convidado, ela será redirecionada para a página de login padrão da Cisco, onde poderá encontrar os botões de login do Google e do Facebook. O usuário pode fazer login usando sua conta Google ou Facebook para obter acesso à Internet.

Etapa 5

Nessa mesma guia, selecione um *Tipo de acesso* no menu suspenso. Neste exemplo, *Login Social* foi selecionado. Essa é a opção que permite que os convidados usem suas credenciais do Google ou Facebook para autenticar e obter acesso à rede.

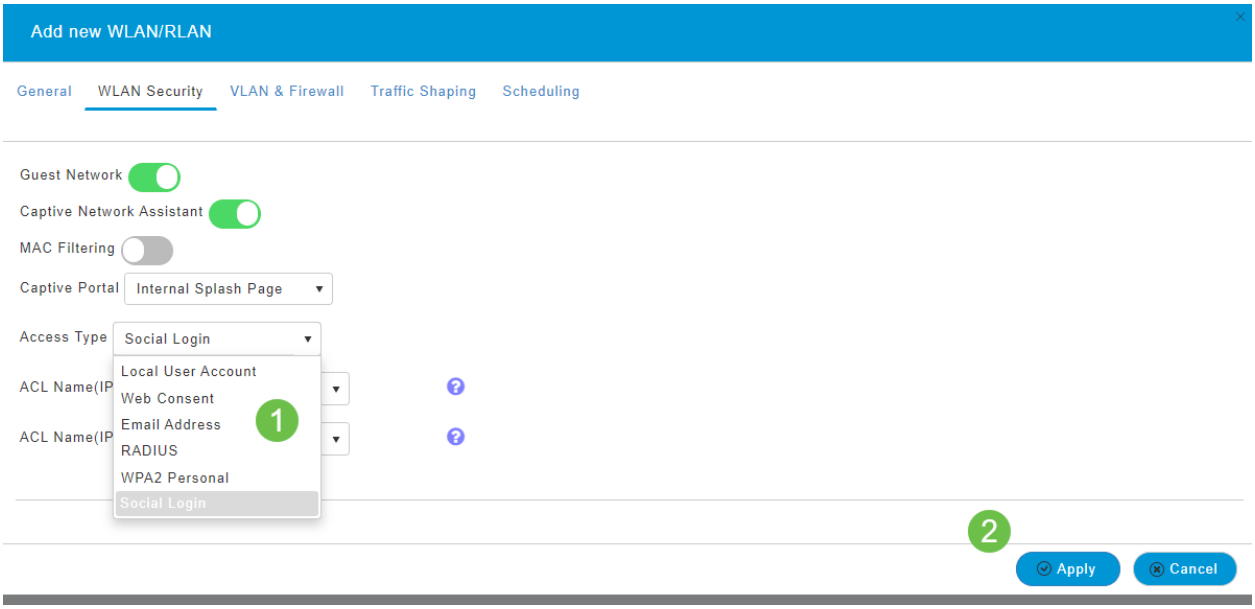
Outras opções para *Tipo de acesso* incluem:

Conta de usuário local - A opção padrão. Escolha esta opção para autenticar convidados usando o nome de usuário e a senha que você pode especificar para usuários convidados desta WLAN, em **Configurações sem fio > Usuários de WLAN**. Este é um exemplo da página inicial interna padrão.

Você pode personalizar isso navegando para **Wireless Settings > Guest WLANs**. A partir daqui, você pode inserir um *Título da página* e uma *mensagem da página*. Clique em Apply. Clique em **Visualizar**.

Consentimento da Web - Permite que os convidados acessem a WLAN após a aceitação dos termos e condições exibidos. Os usuários convidados podem acessar a WLAN sem digitar um nome de usuário e uma senha.
Endereço de e-mail - Os usuários convidados precisarão inserir seu endereço de e-mail para acessar a rede.
RADIUS - Use isso com um servidor de autenticação externo.
WPA2 Personal - Wi-Fi Protected Access 2 com chave pré-compartilhada (PSK)

Clique em Apply.



Etapa 6

Certifique-se de salvar suas configurações clicando no **ícone salvar** no painel superior direito da tela da IU da Web.

Agora, você criou uma rede de convidado disponível em sua rede CBW. Seus convidados vão gostar da conveniência.

Criação de perfil de aplicativo usando a interface de usuário da Web (opcional)

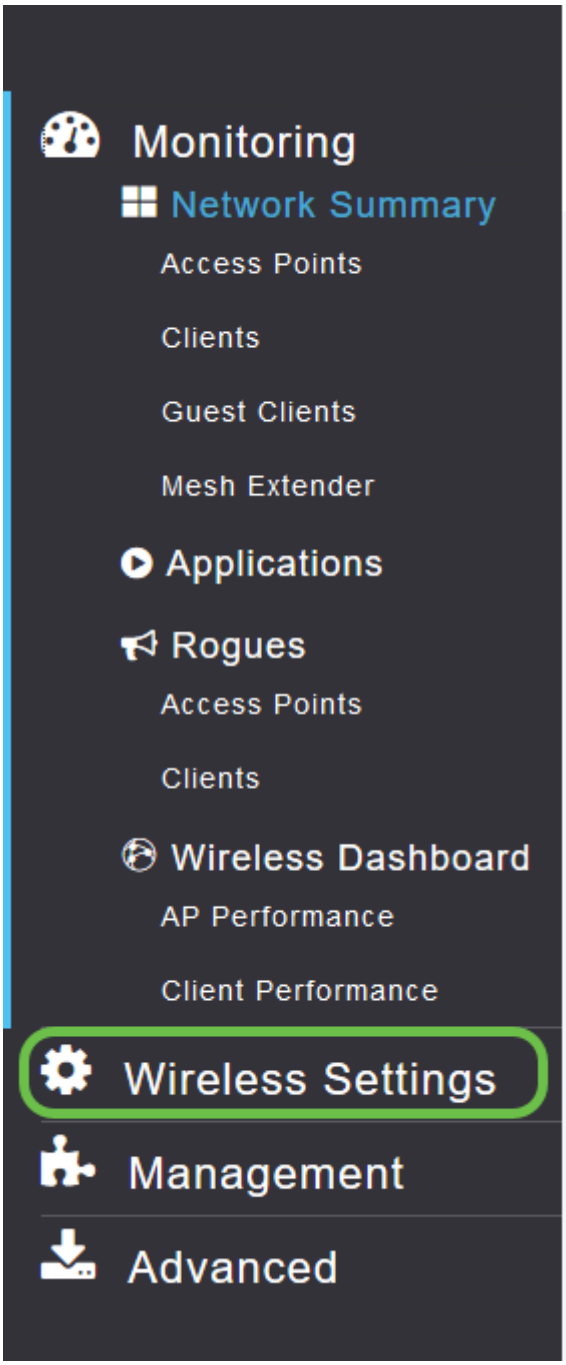
A criação de perfis é um subconjunto de recursos que permite a aplicação de políticas organizacionais. Ele permite que você combine e priorize os tipos de tráfego. Como regras tomam decisões sobre como classificar ou descartar o tráfego. O sistema Cisco Business Mesh Wireless apresenta perfil de cliente e aplicativo. O ato de acessar uma rede como usuário começa com muitas trocas de informações, entre elas o tipo de tráfego. A política interrompe o fluxo de tráfego para direcionar o caminho, como um fluxograma. Outros tipos de recursos de política incluem: acesso de convidado, listas de controle de acesso e QoS.

Passo 1

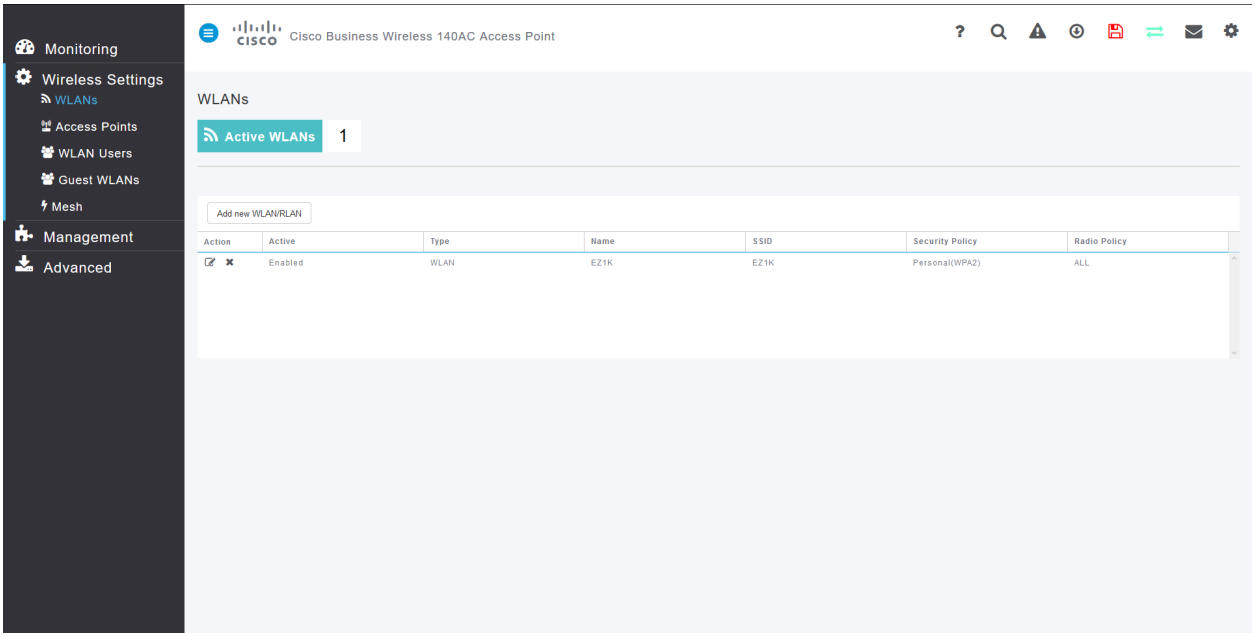
Navegue até o menu no lado esquerdo da tela se não vir a barra de menus à esquerda.

Passo 2

O menu Monitoramento é carregado por padrão ao entrar no dispositivo. Você precisará clicar em **Wireless Settings (Configurações sem fio)**.

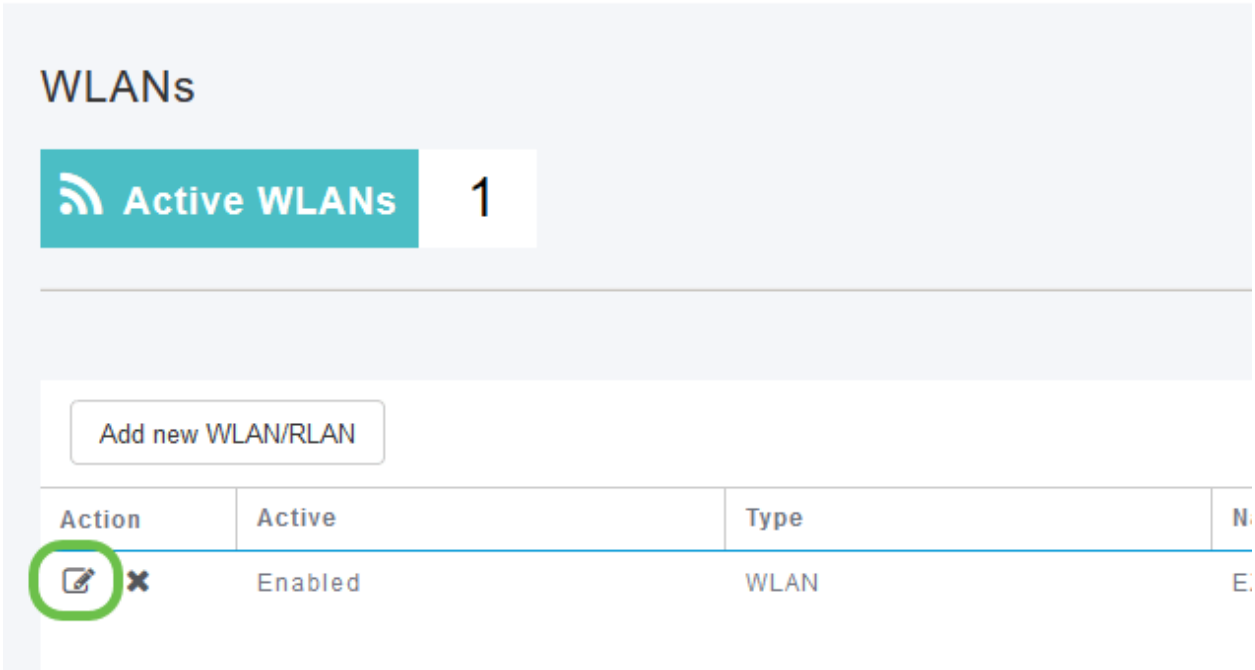


A imagem abaixo é semelhante à exibida quando você clica no link Configurações sem fio.

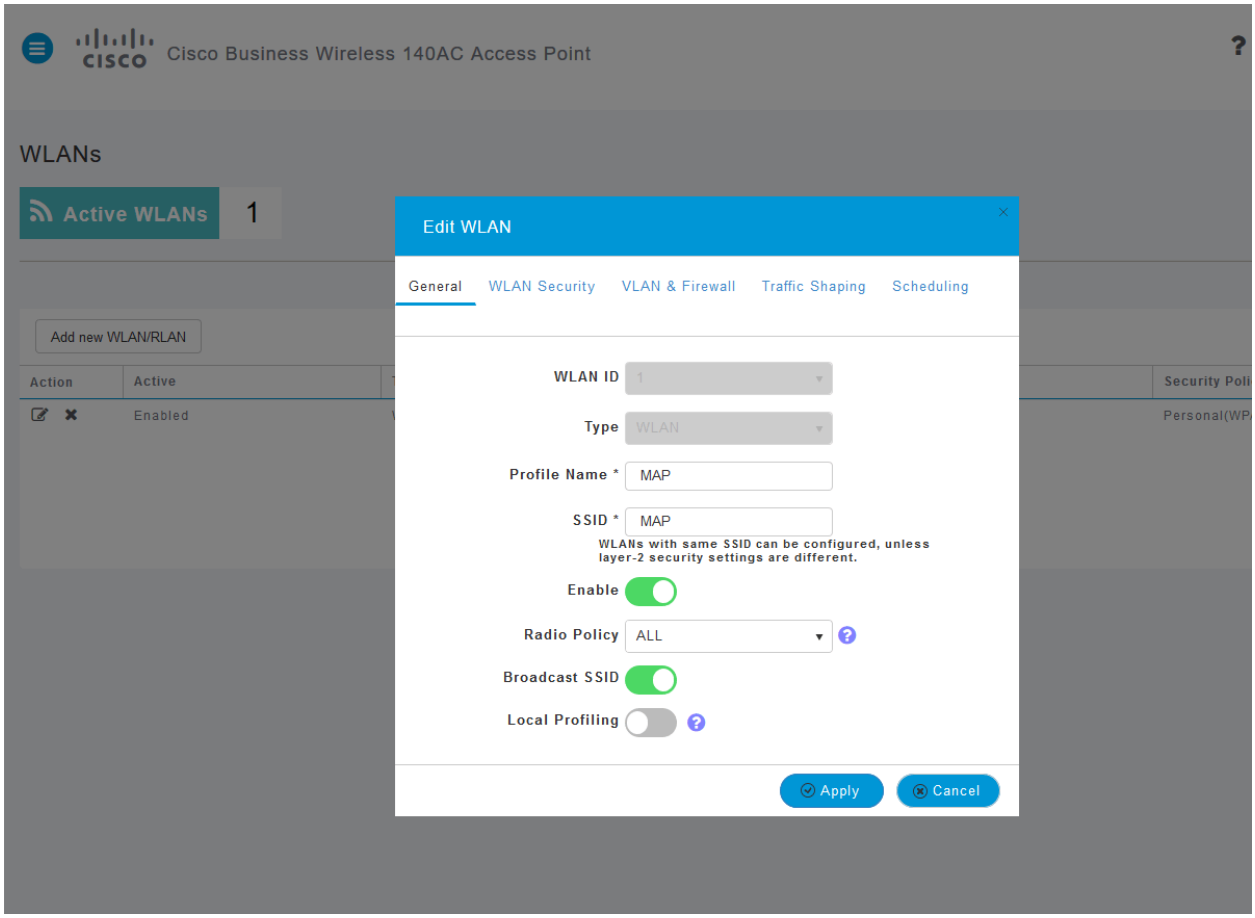


Etapa 3

Clique no **ícone de edição** à esquerda da rede local wireless na qual você deseja habilitar o aplicativo.

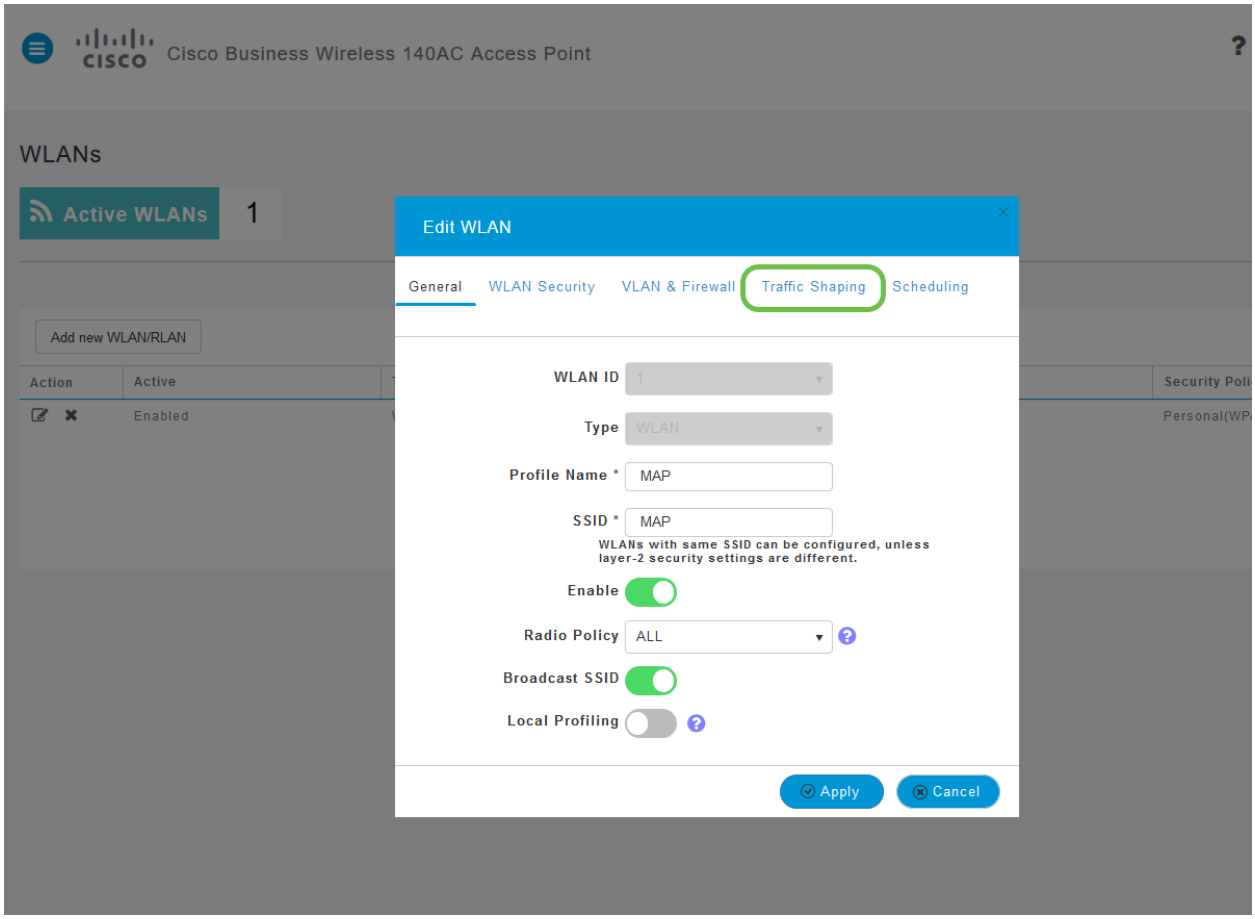


Como você adicionou a WLAN recentemente, sua página *Editar WLAN* pode ser semelhante à seguinte:

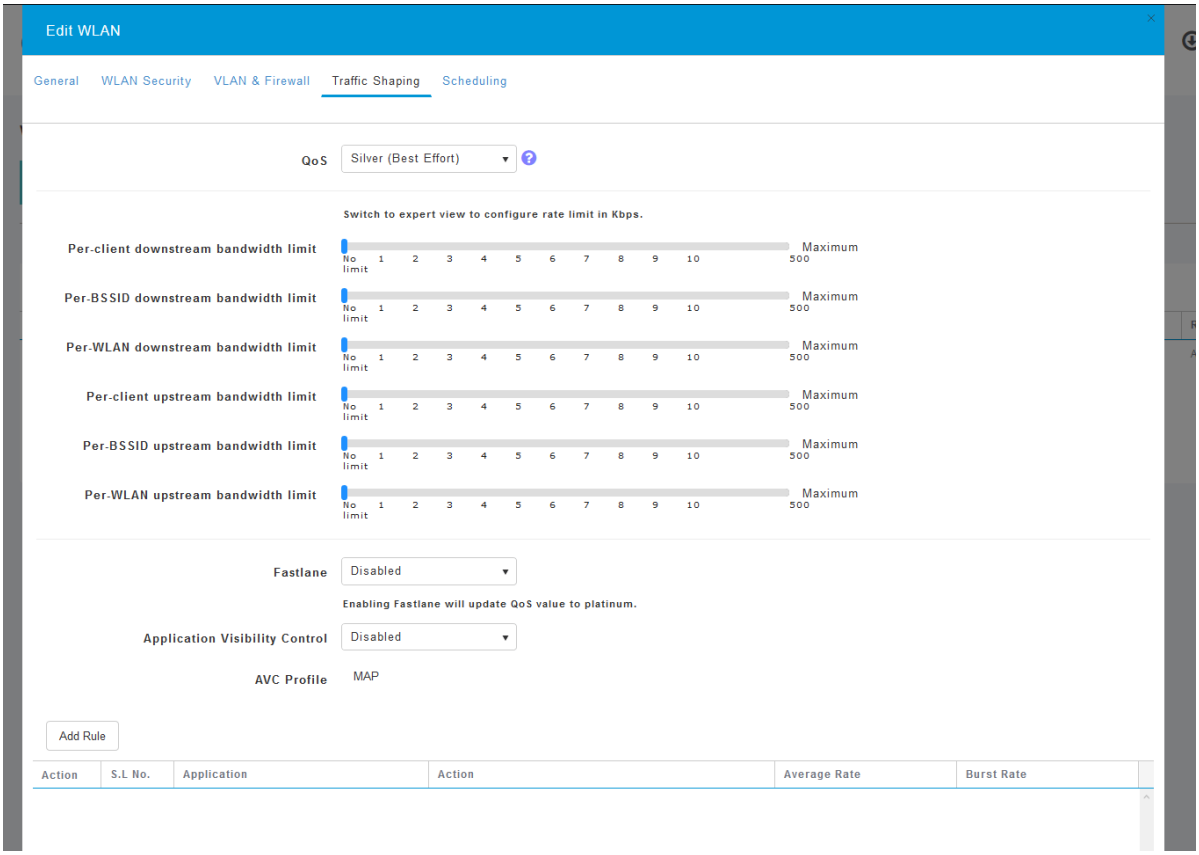


Passo 4

Navegue até a guia **Traffic Shaping (Modelagem de Tráfego)** clicando nela.

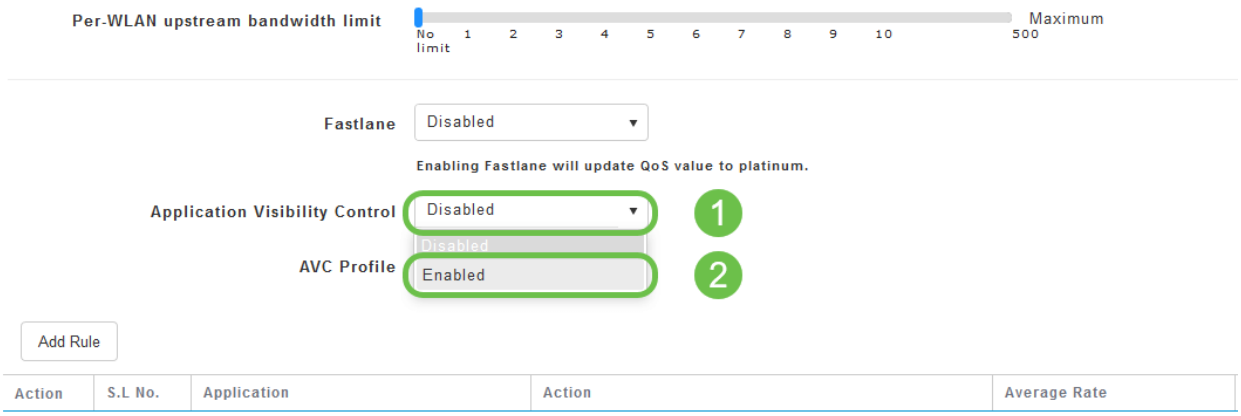


Sua tela pode ser exibida da seguinte maneira:



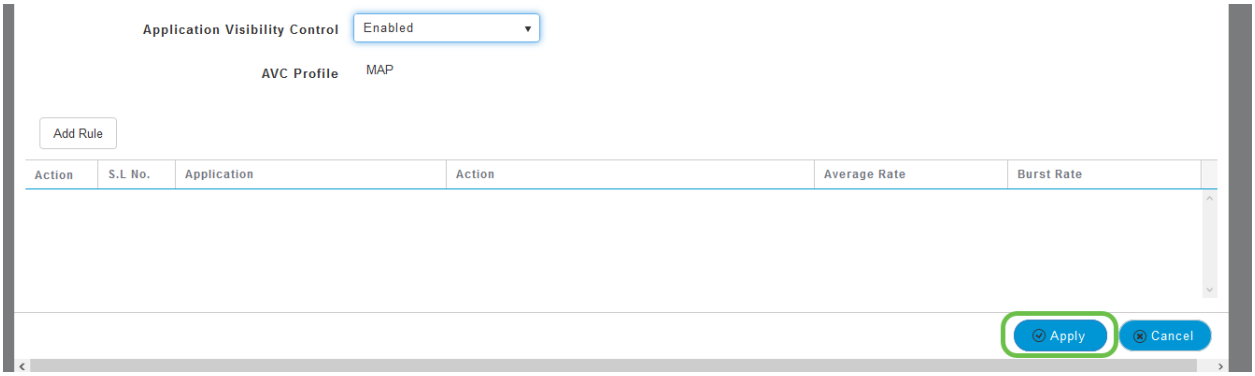
Etapa 5

Na parte inferior da página, você encontrará o recurso *Controle de visibilidade do aplicativo*. Por padrão, isso é desativado. Clique no menu suspenso e selecione **Enabled (Habilitado)**.



Etapa 6

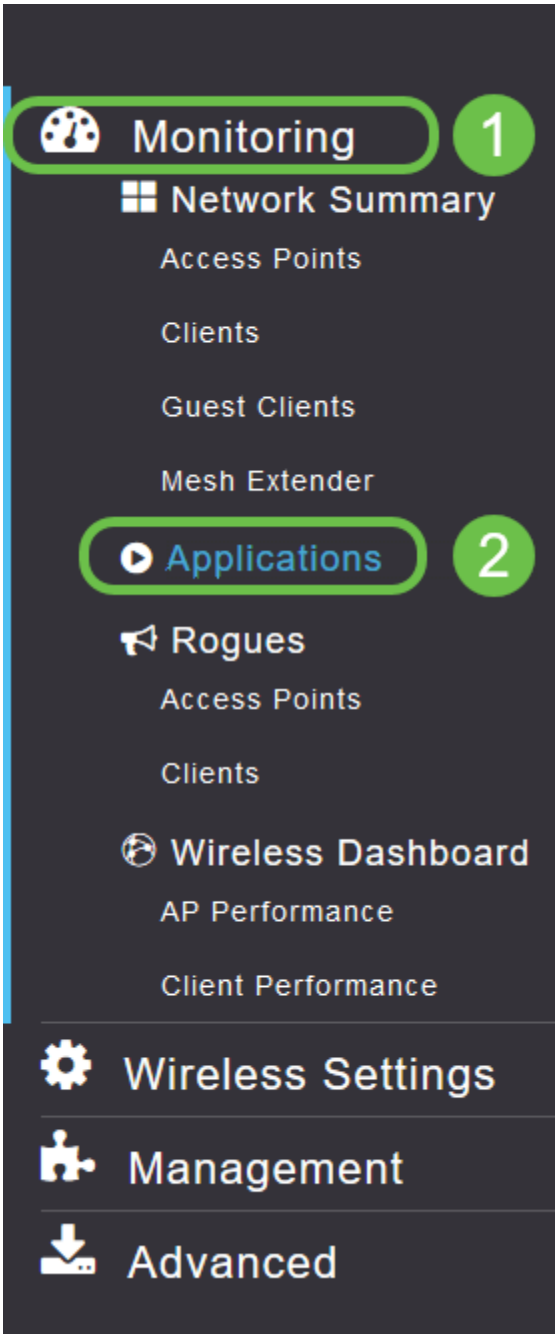
Clique no botão **Aplicar**.



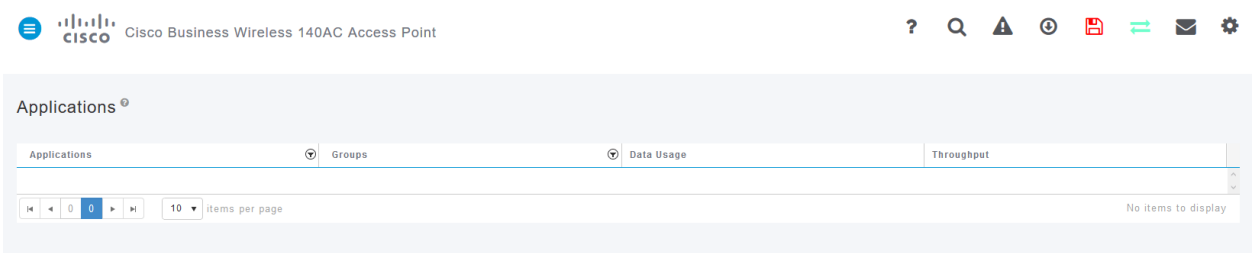
Essa configuração deve ser ativada, caso contrário, o recurso não funcionará.

Etapa 7

Clique no botão Cancelar para fechar o submenu WLAN. Em seguida, clique no menu **Monitoramento** na barra de menus à esquerda. Depois de conseguir, clique no item de menu **Aplicativos**.



Se você não tiver tráfego para nenhuma origem, sua página ficará em branco, como mostrado abaixo.



Esta página exibirá as seguintes informações:

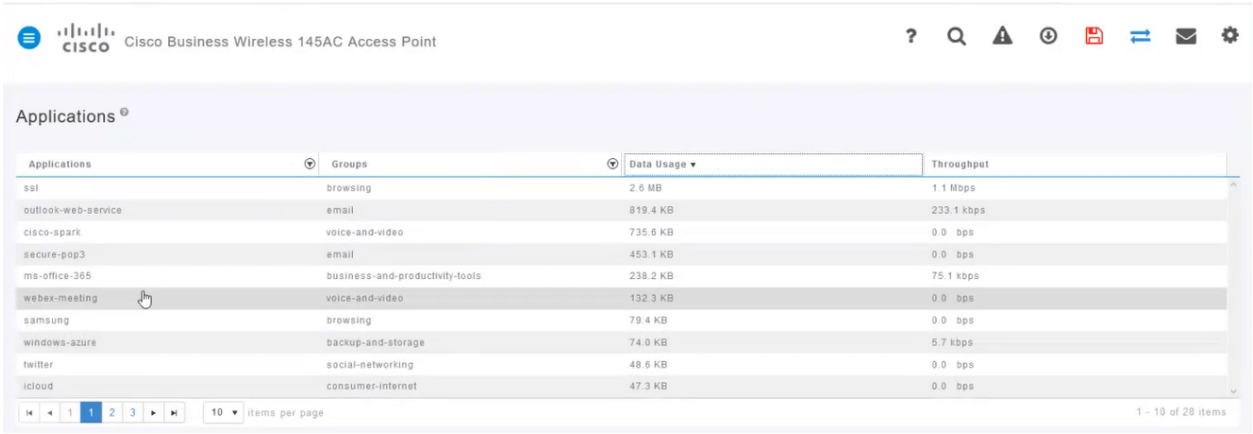
- Aplicativo - inclui vários tipos diferentes
- Grupos - Indica o tipo de grupo de aplicativos para facilitar a classificação
- Uso de dados - A quantidade de dados usada por este serviço como um todo
- Produtividade - A quantidade de largura de banda usada pelo aplicativo

Você pode clicar nas guias para classificar do maior para o menor, o que pode ajudar a identificar os maiores consumidores de recursos de rede.

Esse recurso é muito potente para gerenciar os recursos da WLAN em um nível granular. Abaixo estão alguns dos grupos e tipos de aplicativos mais comuns. É provável que sua lista inclua muito mais, incluindo os seguintes grupos e exemplos:

- Navegação
  - EX: Cliente específico, SSL
- E-mail
  - EX: Outlook, Secure-pop3
- Voz e vídeo
  - EX: WebEx, Cisco Spark,
- Ferramentas de negócios e produtividade
  - EX: Microsoft Office 365,
- Backup e armazenamento
  - EX: Windows-Azure,
- Consumidor-Internet
  - iCloud, Google Drive
- Redes sociais
  - EX: Twitter, Facebook
- Atualizações de software
  - EX: Google-Play, IOS
- Mensagens instantâneas
  - EX: Suspensões, mensagens

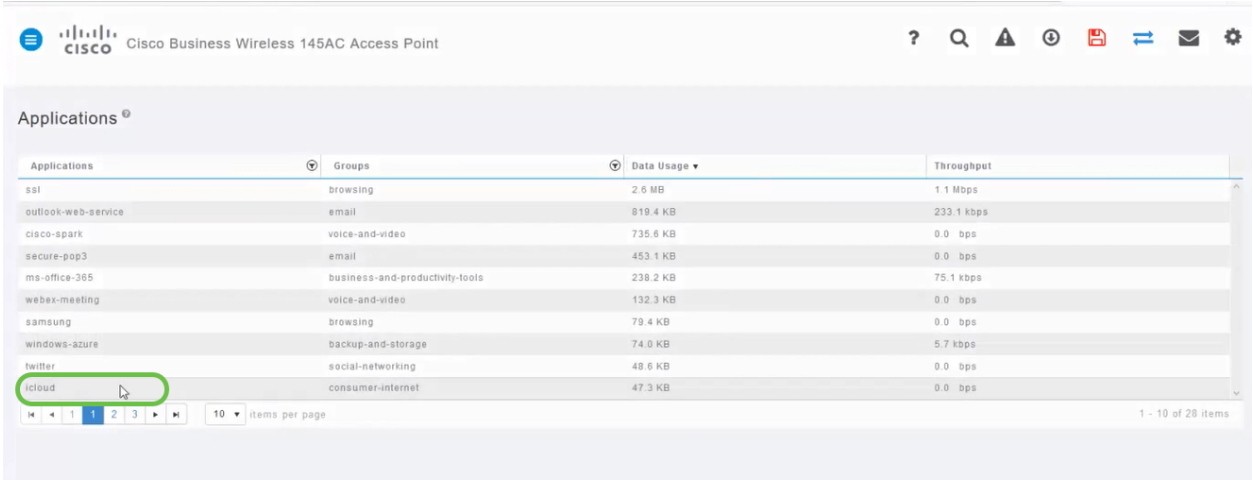
Aqui é mostrado um exemplo de como a página será quando preenchida.



Cada cabeçalho de tabela pode ser clicado para classificação, o que é especialmente útil para os campos *Uso de Dados* e *Rendimento*.

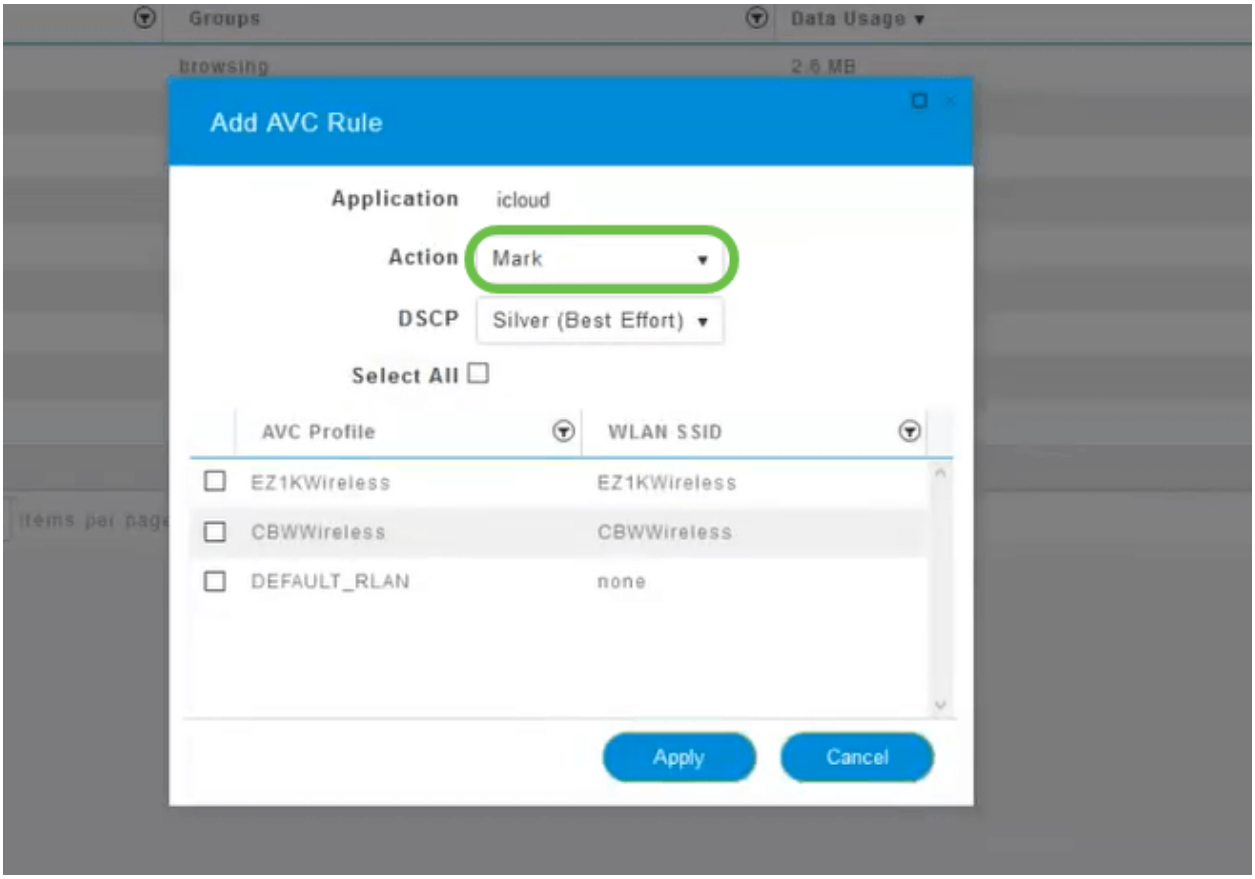
Passo 8

Clique na linha do tipo de tráfego que deseja gerenciar.



Passo 9

Clique na caixa suspensa **Ação** para selecionar como você tratará esse tipo de tráfego.



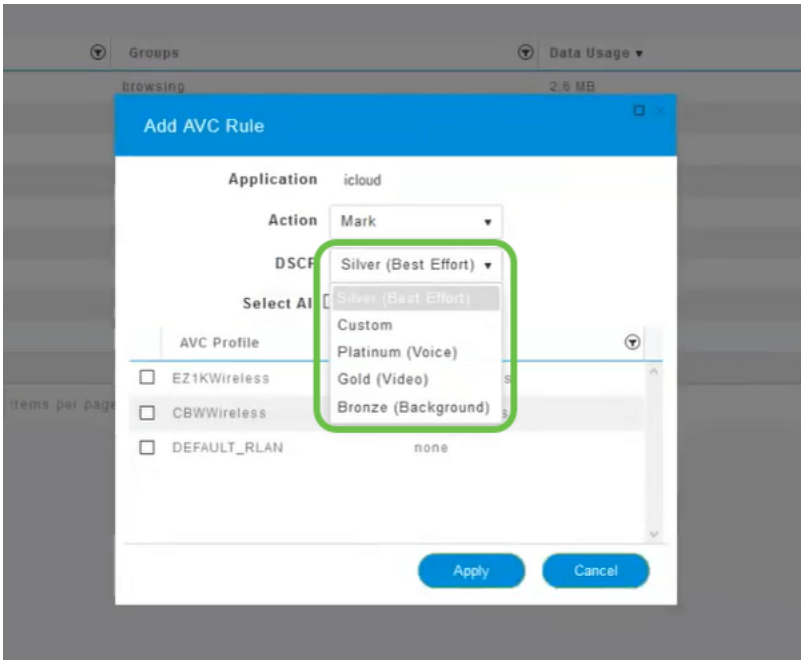
Para este exemplo, estamos deixando esta opção em *Mark*.

Ação a tomar no tráfego

- Marcar - Coloca o tipo de tráfego em um dos três níveis do Differentiated Services Code Point (DSCP) - governando quantos recursos estão disponíveis para o tipo de aplicativo
- Drop - Não faça nada além de descartar o tráfego
- Limite de taxa - Permite definir a taxa média, a taxa de burst em Kbps

Passo 10

Clique na caixa suspensa no campo **DSCP** para selecionar uma das opções a seguir.



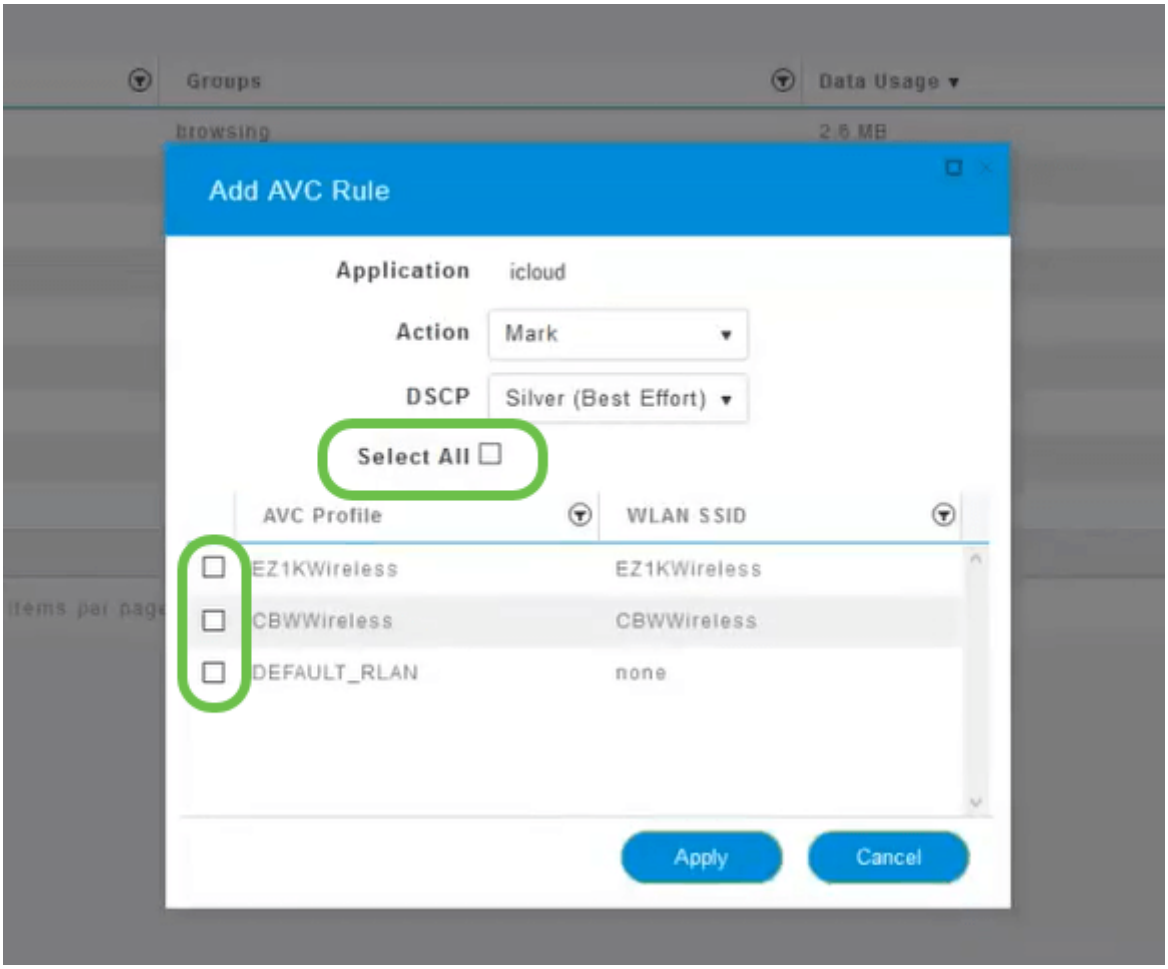
Abaixo estão as opções de DSCP para o tráfego a ser marcado. Essas opções mudam de menos recursos para mais recursos disponíveis para o tipo de tráfego que você está editando.

- Bronze (fundo) - Menos
- Prata (melhor esforço)
- Gold (vídeo)
- Mais Platinum (Voz)
- Personalizado - Conjunto de usuários

Como uma convenção da Web, o tráfego migrou para a navegação SSL, o que impede que você veja o que está dentro dos pacotes à medida que eles se movem de sua rede para a WAN. Como tal, uma grande maioria do tráfego da Web usará SSL. A definição de tráfego SSL para uma prioridade mais baixa pode afetar sua experiência de navegação.

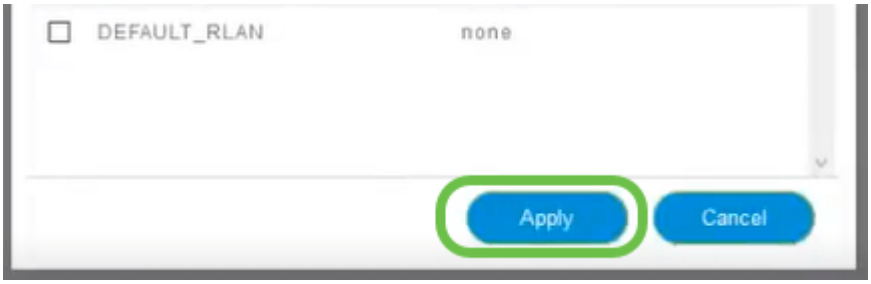
Passo 11

Agora selecione o SSID individual que você deseja que esta diretiva execute ou clique em **Selecionar tudo**.



Etapa 12

Agora clique em **Aplicar** para iniciar esta diretiva.



Dois casos em que tal se poderia aplicar:

- Convidados/usuários transmitindo uma grande quantidade de tráfego, impedindo que o tráfego de missão crítica passe. Você pode aumentar a prioridade de Voz, diminuir a prioridade do tráfego Netflix para melhorar as coisas.
- O download de grandes atualizações de software durante o horário comercial pode ser despriorizado ou a taxa é limitada.

Você conseguiu! A criação de perfis de aplicativos é uma ferramenta muito poderosa que também pode ser ativada com a ativação do perfil do cliente, como detalhado na próxima seção.

Criação de perfil do cliente usando a interface de usuário da Web (opcional)

Ao se conectarem a uma rede, os dispositivos trocam informações de perfil do cliente. Por padrão, o *perfil do cliente* está desabilitado. Essas informações podem incluir:

- Nome do host - ou o nome do dispositivo
- Sistema operacional - o software principal do dispositivo
- Versão do SO - A iteração do software aplicável

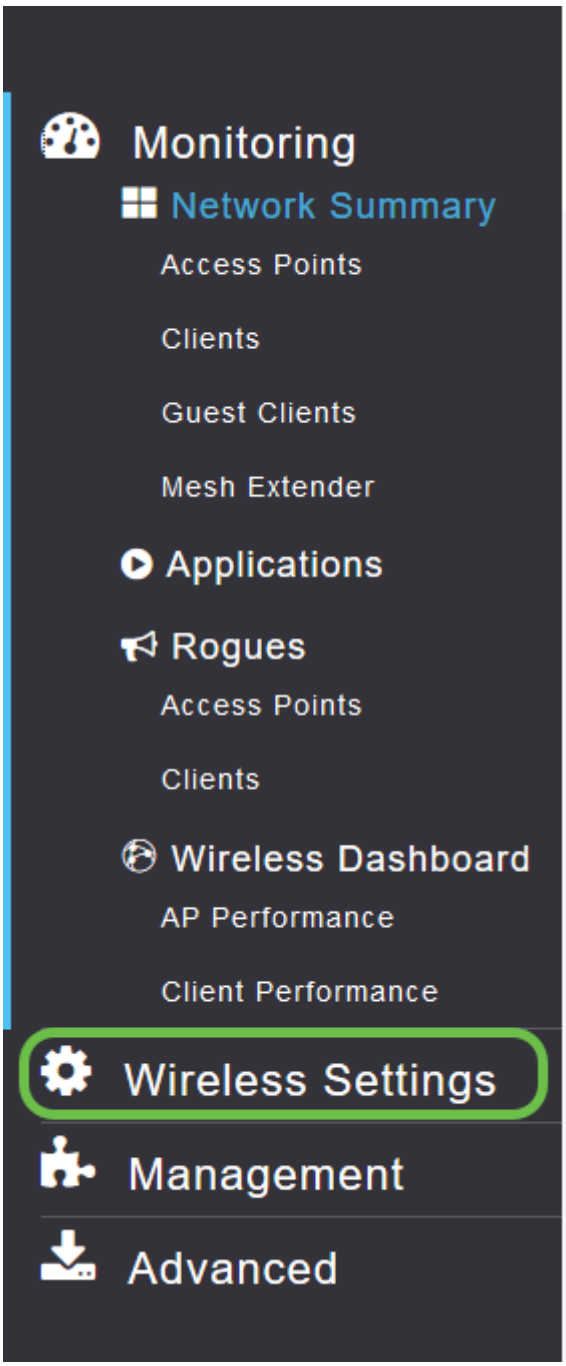
As estatísticas sobre esses clientes incluem a quantidade de dados usados e o throughput.

O rastreamento de perfis de clientes permite maior controle sobre a rede local sem fio. Ou você pode usá-lo como uma função de outro recurso. Como usar tipos de dispositivos de limitação de aplicativos que não transportam dados de missão crítica para sua empresa.

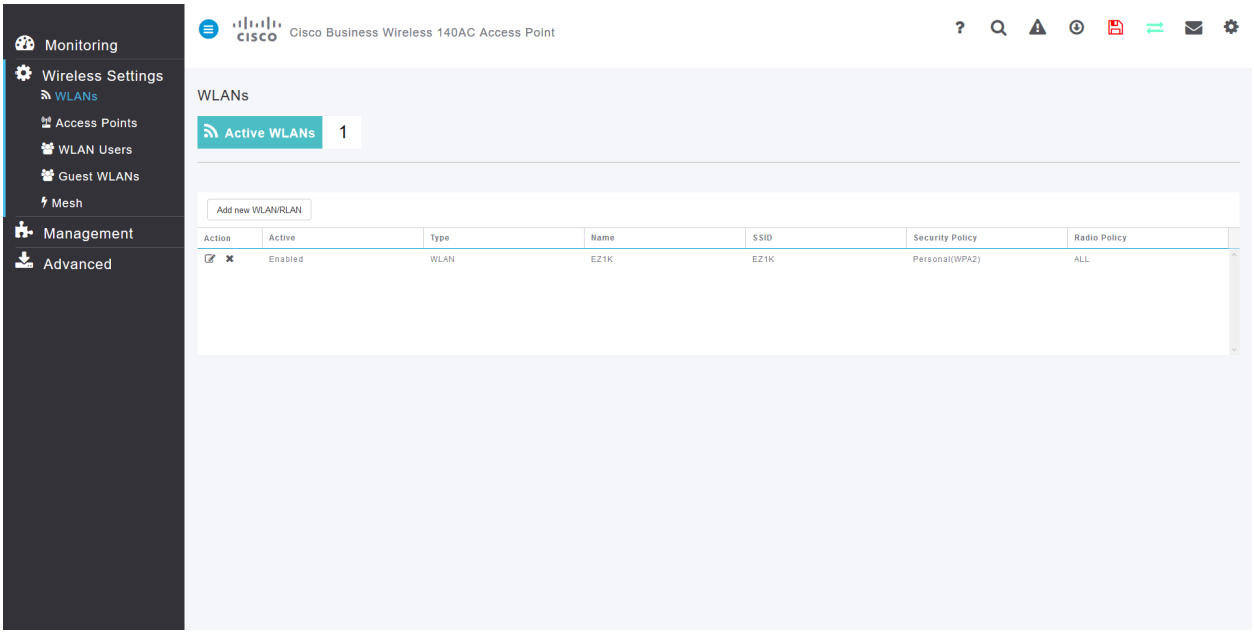
Depois de ativada, os detalhes do cliente para a sua rede podem ser encontrados na seção Monitoramento da interface do usuário da Web.

Passo 1

Clique em **Configurações sem fio**.

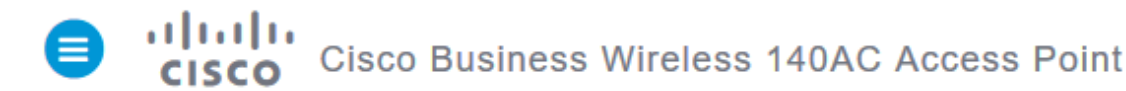


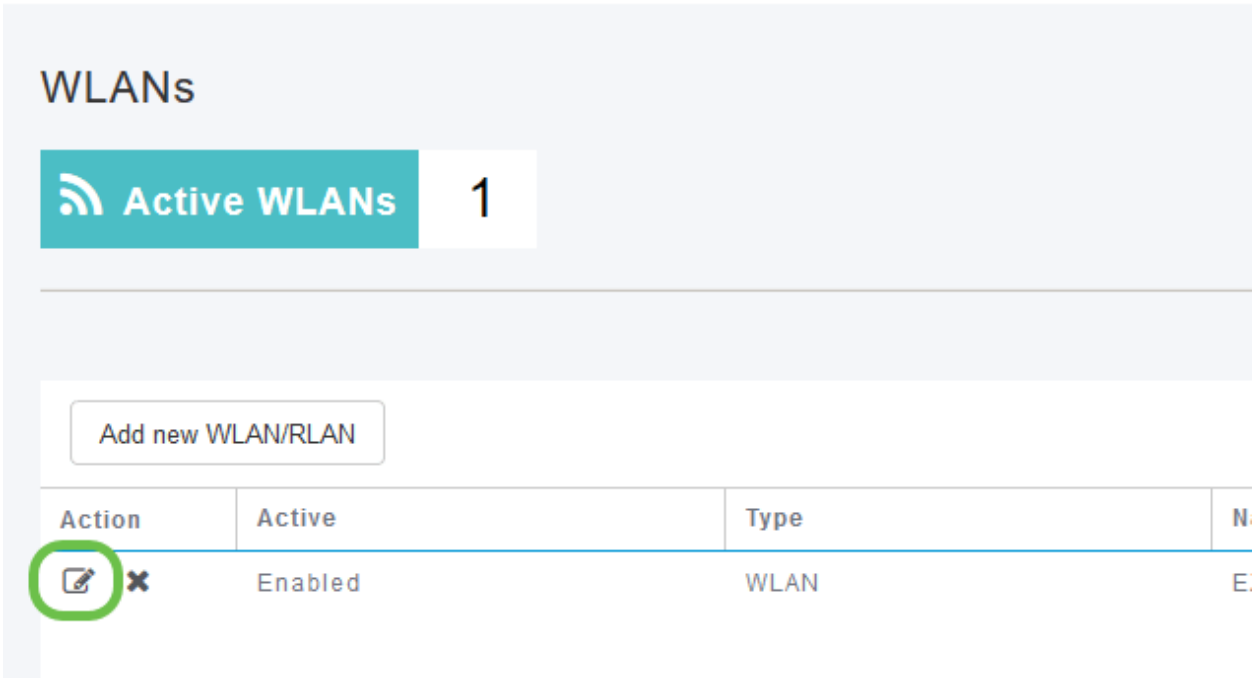
A imagem abaixo é semelhante à que você verá quando clicar no link Wireless Settings (Configurações sem fio):



Passo 2

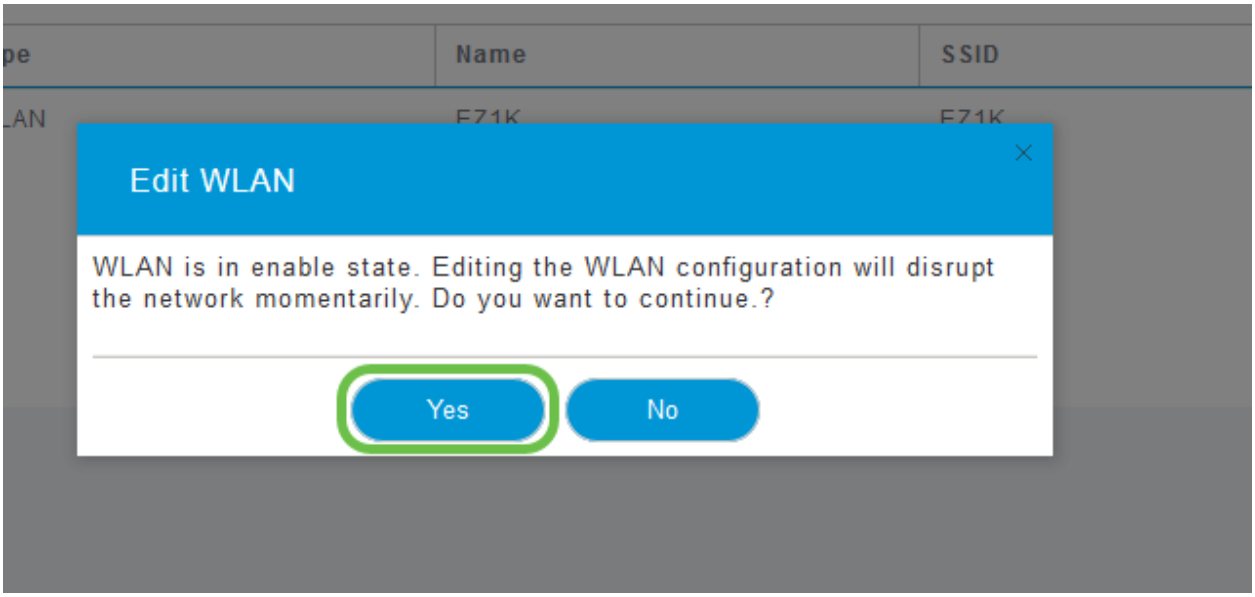
Decida qual WLAN você deseja usar para o aplicativo e clique no **ícone de edição** à esquerda dele.





Etapa 3

Um menu pop-up pode ser exibido de maneira semelhante ao abaixo. Esta mensagem importante pode afetar temporariamente o serviço na rede. Clique em **Sim** para prosseguir.

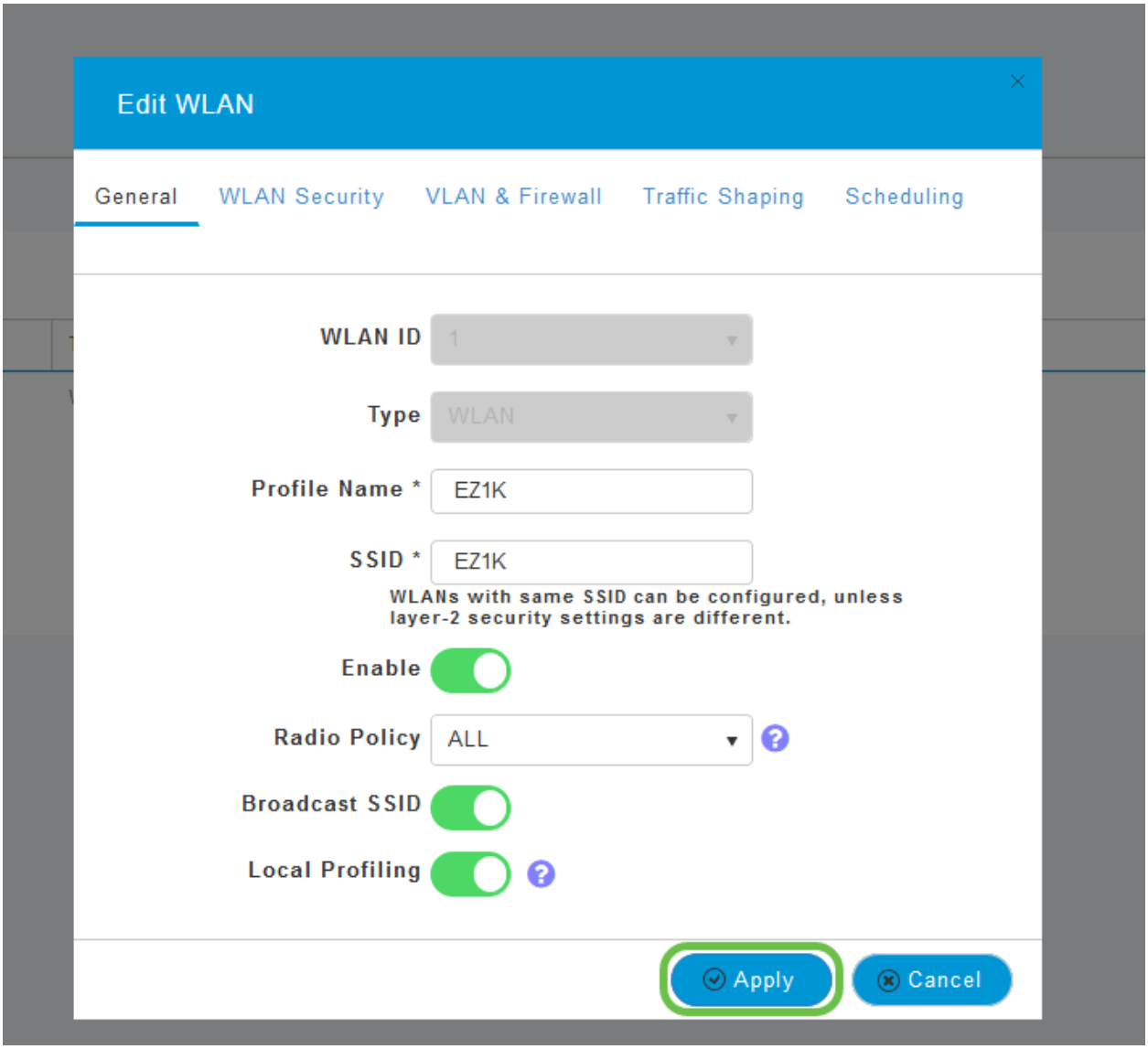


Passo 4

Alterna a criação de perfis de clientes clicando no botão de alternância **Local Profiles**.

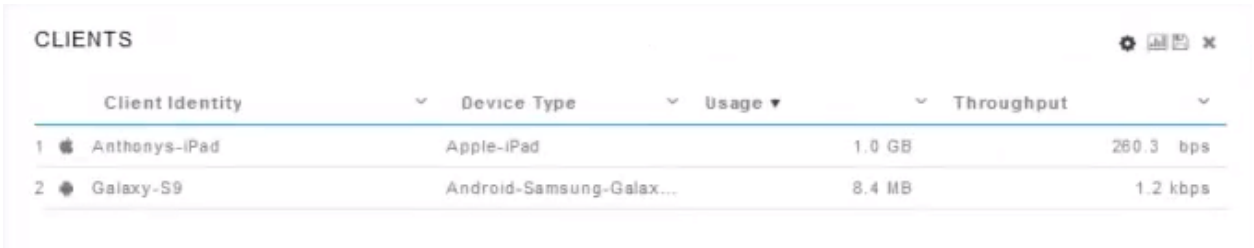
Etapa 5

Clique em Apply.



Etapa 6

Clique no item de menu da seção **Monitoramento** no lado esquerdo. Você verá que os dados do cliente começam a aparecer no Painel da guia *Monitoramento*.



Conclusão

Agora você concluiu a configuração da sua rede segura. Que grande sensação, agora preciso de um minuto para comemorar e depois começar a trabalhar!

Queremos o melhor para nossos clientes, portanto, se você tiver comentários ou sugestões sobre este tópico, envie um e-mail para a equipe de conteúdo da Cisco.

Para ler outros artigos e documentação, consulte as páginas de suporte do seu hardware:

- Roteador VPN Cisco RV345P com PoE
- Access point Cisco Business 140AC
- Extensor de malha Cisco Business 142ACM